Strong Electronic Identification: Survey & Scenario Planning

Oluwabunmi Michael Agbede

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 12.08.2018

Thesis Supervisor:

Professor Raimo Kantola

Thesis Instructor:

Professor Raimo Kantola

Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Agbede Oluwabunmi Michael

Title: Strong Electronic Identification: Survey & Scenario Planning

Date: 12.08.2018 Language: English Pages: viii + 93

Department: Communications and Networking

Professorship: Internet Technologies

Supervisor: Prof. Raimo Kantola

Instructor: Prof. Raimo Kantola

The deployment of more high-risk services such as online banking and government services on the Internet has meant that the need and demand for strong electronic identity is bigger today more than ever. Different stakeholders have different reasons for moving their services to the Internet, including cost savings, being closer to the customer or citizen, increasing volume and value of services among others.

This means that traditional online identification schemes based on self-asserted identities are no longer sufficient to cope with the required level of assurance demanded by these services. Therefore, strong electronic identification methods that utilize identifiers rooted in real world identities must be provided to be used by customers and citizens alike on the Internet.

This thesis focuses on studying state-of-the-art methods for providing reliable and mass-market strong electronic identity in the world today. It looks at concrete real-world examples that enable real world identities to be transferred and used in the virtual world of the Internet.

The thesis identifies crucial factors that determine what constitutes a strong electronic identity solution, and through these factors evaluates and compares the example solutions surveyed in the thesis.

As the Internet become more pervasive in our lives; mobile devices are becoming the primary devices for communication and accessing Internet services. This has thus, raised the question of what sort of strong electronic identity solutions could be implemented, and how such solutions could adapt to the future.

To help to understand the possible alternate futures, a scenario planning and analysis method was used to develop a series of scenarios from underlying key economic, political, technological and social trends and uncertainties. The resulting three future scenarios indicate how the future of strong electronic identity will shape up with the aim of helping stakeholders contemplate the future and develop policies and strategies to better position themselves for the future.

Keywords: Strong electronic identification, authentication, PKI, e-ID cards, Mobile PKI, BankID, Scenario planning & analysis.

Acknowledgements

I am filled with utmost gratitude towards Professor Raimo Kantola for accommodating me and supporting me through the course of writing this thesis. His advice and careful guidance have been a light in my path throughout my studies at Aalto.

I would also like to extend my gratitude to my colleagues at Methics Oy. You guys have been amazing; you cannot imagine how great of a help you have been to me in the course of writing this thesis. Our discussions and your answers to my sometimes-ignorant questions provided me with the needed tools to complete this thesis.

I especially thank my parents who have always encouraged and supported me in every stage of life. Finally, I would like to thank my sisters and friends who have all added value and brought beauty to my life.

Espoo, August 12, 2018

Oluwabunmi Michael Agbede

Abbreviations and Acronyms

AP	Application Provider
API	Application Programming Interface
CA	Certification Authority
CRL	Certificate Revocation List
e-ID	Electronic Identity
eIDAS	Electronic Identification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
ETSI TR	ETSI Technical Reports
ETSI TS	ETSI Technical Specifications
EU	European Union
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
ID	Identity
ISO	International Organization for Standardization
LoA	Levels of Assurance
MNO	Mobile Network Operator
MSS	Mobile Signature Services
MSSP	Mobile Signature Service Provider
NFC	Near-field communication
OCSP	Online Certificate Status Protocol
OTP	One-Time-Password
PII	Personal Identifying Information
PIN	Personal Identification Number
PKC	Public Key Cryptography

PKI	Public Key Infrastructure
PSD2	Payment Services Directive 2
QESCD	Qualified Electronic Signature Creation Device
RA	Registration Authority
RFID	Radio-Frequency Identification
RP	Relying Party
SE	Secure Element
SSN	Social Security Number
STK	SIM Toolkit
TAN	Transaction Authentication Numbers
TEE	Trusted Execution Environment
WPKI	Wireless Public Key Infrastructure

Contents

List of Tables and Figures

List of Figures

List of Tables

Chapter 1

Introduction

Today, a person's ability to prove their identity is seen as an important basis for participation in the society and life in general. In most countries around the world, establishing a person's identity whether online or offline, is critical to accessing a wide range of services, including education, healthcare, voting, banking, mobile communications, housing, etc. [3], [81], [82].

Over the last couple of years, we have seen a gradual shift in the provision of services by businesses, financial institutions, governments etc. from physical face-to-face interactions to Internet-based interactions. This evolution is expected to continue over the next couple of years and we can relatively expect most of the current face-to-face services to become completely web-based in the future. Factors driving this evolution include, convenience, cost, and the proliferation of cheap Internet connected devices among the populace, as well as the maturity of web technologies. The proliferation of smartphones has meant that we can access web services at any place, at any time. The increased mobility and Internet connectivity has driven the demand for digital services from a sort of "Additional service" offered by service providers to become a critical requirement for achieving success in business or government service delivery. High risk services like e-Government, e-Health and e-Banking have become mainstream, thus the rise in the demand for strong assured person identification on the Internet [3].

In the early days of the Internet, the idea was that anyone could be anything he or she want to be on the Internet, completely separate from who he or she is in the real world. There was even a saying that "on the Internet, no one knows you're a dog", arising from a Peter Steiner cartoon published in The New Yorker on July 5, 1993[1] [2]. The time when this statement is valid, is well and truly over. [2] The number of applications we now access via the web, which would ordinarily require our physical presence, have meant that some service providers require a reliable way to identify and ascertain that a person is indeed who they claim they are. In other words, a real person cannot exactly claim to be a dog; of course, you are not prevented from

---

[1] *Wikipedia. "On the Internet, nobody knows you're a dog." Retrieved from: https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog (Accessed 08/11/2017)*

[2] *Aleks Krotoski. "Online identity: is authenticity or anonymity more important?" The Guardian [Internet] Thursday 19 April. Retrieved from: https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity. (Accessed 08/11/2017).*

claiming whatever identity, only that to access services requiring strong identity assurance, a person claiming to an identity must be able to back that claim up before they would be granted access [1], [2].

According to Wikipedia[3], Identification allows an unknown person or entity (subject) to become known (i.e. identified). Identity refers to a set of attributes that can uniquely identify a person [1], [6], [13]. Physical world identification could be done by presenting physical identification credentials such as Passports, Driving licenses, National ID cards etc. These normally contain some sort of personal identifying attribute including name of the owner and some authenticating information such as a signature and/or photograph, which is easily verifiable to stop them being used by someone other than the person to which it was issued [4], [28].

In a digital Identity system, "identity" refers to a set of attributes digitally stored that represents a person or entity.[4] Bringing the identification and identity definitions together, a digital identity can be defined as a collection of identifying attributes that uniquely describe a person electronically stored to be used on the Internet and for electronic transactions.[5] Today, citizen identity documents are still very much physical; such documents are becoming obsolete as services move to the Internet. Transferring identity solutions and verification processes onto the Internet has not been smooth or fast enough, as we would expect, even though many governments and enterprises have come up with different solutions with varying degrees of success [4].

For some services on the Internet, anonymity and privacy would continue to be an important requirement, however high risk services such as financial services and e-government services will continue to require trusted identification solutions that assure a unique match between the person online and the person in the physical world [30].

1.1. Motivation

Initially, the Internet was developed and seen as a tool for communication in the academia and with the assumption that every actor is a good actor and could be trusted. In fact, the designers of the Internet could never have envisaged its pervasion in our lives today. It is common to do everything today on the Internet including shopping, banking, e-education, access government services etc. The application of the Internet today is endless, it makes life easier, and for the businesses or the government, the web provides a cheaper, easier and faster access to consumers/citizens.

Therefore, today, identification of communication partners is more important than ever. The assumption that everyone on the Internet would behave in a fair and ethical manner is

[3] Wikipedia. "*Identification (Information).*" Retrieved from: https://en.wikipedia.org/wiki/Identification_(information). (Accessed 08/11/2017)
[4] Wikipedia. "*Electronic identification.*" Retrieved from: https://en.wikipedia.org/wiki/Electronic_identification. (Accessed 08/11/2017)
[5] *Electronic Identities: A brief introduction.* Retrieved from: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf

completely out of date and touch with present day realities. As the adoption of the Internet has exploded, so have the number of cybercrimes, leading to a need to protect people, devices etc. on the Internet. A strong linkage of electronic identities to real people has the ability to reduce many forms of cybercrime.

The major challenge is how do we ensure a reliable and trustworthy match between an online identity and a physical one? An online identification solution with a substantial Level of Assurance (LoA) should be able to achieve a similar level of trust and acceptance as a trusted identity document used in the physical world. In any case, the source of the identity must be trusted within the domain/realm of identification and that is why we have seen governments playing an important role, both in legislation, issuance, certification and regulation of identity documents and providers [3], [4], [46].

There have been several attempts at ensuring that someone online is the same person offline. Internet giants such as Facebook and Google have made it a policy by requiring that a profile created on their platforms be attached to a real person.[6] Also, the mass collection of data about their users (including user attributes like name, address/location, behavior patterns including likes and dislikes, interactions and date of birth), allows these platforms to link the captured data/attributes to a real person to a relative degree of certainty. These have enabled these companies to become Identity Providers (IdPs) through a combination of technologies and protocols such as OAuth, OpenID, SAML, etc. Unfortunately, since these solutions were designed to solve the authentication problem, they cannot be strong assured to meet the identification requirements for high risk services. The identities they provide are based on self-asserted attributes that could be incorrect, based on pseudonyms or deliberately faked. This is because there isn't any sort of identity verification built into the registration processes of the platforms (except confirming your email address, which could in itself be based on a false data), therefore, these solutions just about come short as offering a credible strong identification solution. This has meant that identity provided is only useful for services requiring lower levels of identity assurance [11], [13].

The primary motivation for this thesis is to survey examples of reliable and strong electronic identity solutions that have been implemented for person identification on the Internet. It looks at concrete solution examples to understand how unique official real-world citizen identities could be transferred and used in the virtual world of the Internet.

As more and more societies are seeking to implement strong electronic identity, it is crucial for policy makers and industry stakeholders to have access to resources for their decision making. This thesis seeks first to understand various technology options available for implementing mass-market strong electronic identities. It presents technical and non-technical factors as well as constraints affecting each strong electronic identity solution, such that stakeholders could make the right decisions given their specific conditions and unique environments. The strong electronic identity solutions identified in this thesis are surveyed in terms of what entities are found in each solution, what connections exist between the entities, the service flow between

[6] Aleks Krotoski. *"Online identity: is authenticity or anonymity more important?"* The Guardian.

the entities to both establish and use strong electronic identities. It also crucially studies how a strong electronic identity is established, managed, and used on the Internet.

Further, in the constantly changing technological landscape, technologies and solutions today might not be acceptable in only a few years, another motivation of this thesis is to study and understand the possible future landscapes of strong electronic identity based on identified key trends and uncertainties affecting the industry. The study conducted by this thesis is intended to provide a valuable information resource to policy makers and stakeholders who might want to understand what alternative futures could be contemplated and suitably position their investments, assets and policies to better manage alternate futures.

In summary, this thesis seeks to answer the following research questions:

- What is strong electronic identification?
- What are the technologies available that could be used to implement mass-market strong electronic identities?
- What are the possible future scenarios for delivering strong electronic identities?

1.2. Scope

The concept of identification and electronic identity is rather broad and as described in the earlier sections of this thesis, covers a wide range of digital identity solutions used on the Internet. In this thesis, we are interested in only strong electronic identity solutions, i.e. digital identity solutions that can confidently answer the questions of "who are you?" and "are you who you claim to be?" on the Internet [47]. The solution must also present an answer to the question of how do we ensure that for services that require strong identity assurance, a person's online identity is the same as their physical identity? [3].

To define and limit the scope of the thesis, the solutions surveyed have been selected based on the following criteria:

1. A digital identity solution is a "Strong electronic identification" solution as defined by the Finnish Act on Strong Electronic Identification and Electronic Signatures [7] and/or "Advanced Electronic Signature" according to the European Union's Electronic Identification and Trust Services (eIDAS) regulation [8].

2. The solution should offer a "High Level of Assurance" in the identity provided as defined in the European Union's Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification [9] and/or LoA4 in the ISO/IEC 29115:2013 [15] standard definition.

3. The solution could be usable to produce electronic signatures that could have the same legal standing as a handwritten signature [8].

From the three selection criteria listed above, this thesis will survey three strong electronic identification solutions.

1. Smartcard based physical e-ID cards commonly found in national e-ID schemes,
2. UICC/SIM card based Mobile Identity (Mobile PKI/ID) Solution, mostly managed by MNOs, and
3. Different implementations of BankID, which is an electronic identity solution based on banking credentials. The BankID survey would include for example, the Finnish bankers' association's offering, called TUPAS, which is a less assured solution but one that is widely accepted in Finland. TUPAS has proved popular among subscribers with higher adoption rate than any other solution and have thus, led to the Finnish government designating it as an acceptable solution for strong electronic identification [5].

The three implementation technologies or approaches listed above account for some of the most popular and successful electronic identification solutions on the market today. The three have been chosen solely at the discretion of the author based on the defined criteria and thus, some other equally secure but proprietary solutions have been left out.

1.3. Methodology

This thesis uses a research methodology based on literature survey of academic and research publications, key industry insights in the form of industry white papers, technical reports and expert discussions with stakeholders. The structure of the thesis reflects the detailed methodology employed in the survey of solutions and corresponding scenario planning and analysis.

The three identified solutions are surveyed based on information from literature and Internet research, with scientific publications, industry white papers and case studies serving as relevant sources of information.

To contemplate and better understand the possible alternate futures of strong electronic identification, a scenario planning and analysis[7] is completed. A scenario planning method based on the identification of key trends, uncertainties and the interrelationships between them is used to construct future scenarios as tools for imagining how strong electronic identification on the Internet in the future might unfold [12]. The Scenario planning and analysis method is described in detail in Chapter 7.

1.4. Thesis outline

The thesis is divided into following chapters.

The background chapter looks at the literary background of Identity and identification. An in-depth perspective on identification is presented, including identification in the physical world, what constitutes a digital identity and strong electronic identification. Levels of Assurance (LoA), Authentication, Authentication factors and methods of implementing authentication are

[7] Wikipedia. "Scenario analysis" Retrieved from: https://en.wikipedia.org/wiki/Scenario_analysis. (Accessed 28/07/2018)

also reviewed. PKI as an important foundation for strong electronic identification is explored, with a study of public key cryptography standards and terms such as digital certificates and signatures. Finally, the chapter ends with a review of common applications of strong electronic identities.

Chapter 3 surveys physical e-ID cards, which are strong e-ID implementations based on smartcards commonly found in citizen identity implementations by the Government. This form of e-ID solution uses physical tamper-resistant smartcards as the secure element for storing citizen attributes and digital certificates. Important technical, security and privacy features of smartcards that make them suitable as qualified electronic signature creation devices (QESD) for strong electronic identity are studied. The chapter also reviews service architecture of this form of e-ID solution, identifying important stakeholders as well as their roles in the e-ID infrastructure. A typical service (usage) flow of an e-ID card is also presented. The chapter ends with a review of example implementations, along with their market penetration and typical use cases and finally limitations common to strong e-ID implementations based on physical e-ID cards.

Chapter 4 surveys another strong electronic identity solution implemented completely on mobile devices, otherwise referred to as mobile signature service, Mobile PKI or Mobile ID. The chapter begins with an introduction to Mobile Signature Service (MSS), identifying the key technical and security features required on UICC/SIM cards to delivery strong electronic identity in Mobile PKI. The chapter also reviews the Mobile PKI service concept and architecture, identifying key stakeholders and their roles, as well as how Mobile PKI is generally implemented. The chapter ends with a review of an example implementation, its market penetration, typical use cases and limitations common to Mobile PKI implementations.

Chapter 5 surveys BankID which is an electronic identity certification service provided by some banks. BankID typically involves the use of bank credentials by customers to identify and authenticate on third-party service provider platforms. This chapter studies what BankID is according to literature, the different approaches taken to implement it in different markets and overall service infrastructure. The chapter surveys real world examples of BankID implementations, their technical features, market penetration and finally weaknesses found in the surveyed BankID implementation examples.

Chapter 6 compares the surveyed solutions in Chapters 3, 4 and 5 based on a number of defined criteria, including technologies the solutions are based on, security architectures, perceived privacy protection, supported use cases, levels of assurance provided by the solution among others.

The Scenario planning and analysis chapter explores the key trends and uncertainties affecting or are likely to affect strong electronic identity solutions and constructs a series of possible scenarios for the future based on interrelationships between the trends and uncertainties.

Chapter 7 discusses the main conclusions of the thesis.

Chapter 2

Background

Identification is the process of making known what and who an entity is; it combines processes that make it possible to proof that an entity is who it claims it is. This involves using some credentials against a claimed identity, to infer who the individual really is. Throughout history, Identification whether based on an individual's innate characteristics (e.g. facial recognition, fingerprints or other biometrics) or some external credential, has facilitated participation in the economic, social and political dimensions of the society. Today, the secure and reliable identification of a person is a key precondition for granting access to various societal resources [22]. Strong electronic identity solutions provide several functions including fraud prevention, enable access to socioeconomic services, allow quick background checks, proof of age, proof of citizenship, generating electronic signatures, among others, all crucial to a functioning and equitable society.

Strong identification of an entity requires the authentication of its identity, which is the process of establishing a level of confidence that the claimed identity does indeed refer to the specific entity making the claim [6]. According to [24], identity authentication happens in two phases:

1. An identification phase, during which an identifier to be authenticated is selected, and
2. An authentication phase, during which the required level of confidence is established (often by challenging the individual to present credentials supporting the identity claim).

The identity authentication process relies on a set of characteristics or attributes (identifiers) that uniquely distinguish the claimant from another person. By default, the identification of a person begins at birth by the state (or government) where they are born. The first step in validating the newborn's identity is achieved by the issuance of a birth certificate, which among other attributes collect the date of birth, birth name, parent's information, unique social security number etc. Typically, these identifiers stay the same over the lifetime of the person and constitute what is referred to as personal identifying information (PII).

2.1. What is Personal Identifying Information (PII)

According to Camp [17], an identifier distinguishes a distinct entity within the context of a specific namespace. These include attributes associated with an entity, which could be used to identify or describe the entity. Thus, Person Identifying Information/Attributes (PII/A) are unique attributes or identifiers which could be used to uniquely identify a person. According to NIST Special Publication 800-122 [16], Person Identifying Information is:

1. Any information that can be used to distinguish or trace an individual's identity, and
2. Any other information that is linked or linkable to an individual.

In the EU, all data concerning a person are covered under the European Union's definition of Personal Data. The EU's General Data Protection Regulation (GDPR) [14] defines Personal data as "Any information related to a natural person or 'Subject' that can be used to directly or indirectly identify the person".

Some examples of personal identifiers according to the definitions in the EU's GDPR and NIST Special Publication 800-122 documents are presented below.

Primary PII.

- **Name**, such as a person's first name and last name (or full name), maiden name, etc.
- **Personal identification number**, this includes uniquely identifying numbers such as a person's social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, etc.
- **Personal characteristics,** this refers to inherence data (i.e. physical, biological features/attributes) about a person that can be captured and/or measured. This includes photographic image (e.g. of face), fingerprints, or other biometric data (e.g., retina scan, voice signature, facial geometry), etc.

The PII or personal data identified by both publications also includes data which alone may not be enough to identify a person but which when linked or referenced along with other data make it possible to identify a person. Examples include:

- Location Information, this refers to address information of a person, such as home address, email address, IP/MAC addresses etc.
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, employment information, medical information, education information, financial information etc.).
- Telephone numbers, including mobile, business, and personal numbers
- Information identifying personally owned property, such as vehicle registration number or title number and related information

PII as presented in the examples above, consist of identifiers associated with a person that are based on attributes that are difficult and/or impossible to alter [17]. Today, the most important PIIs in most countries, include social security numbers, name, age (or date of birth) and physical address.

The collection of PII in either physical identity documents or online digital certificates provides the assurance that services where it is critical to know the identity of a person are accessed or delivered to the persons to which it was intended.

2.2. Identification in the physical world

Identification in the physical world is required in cases where a person must be identified to establish trust. The trust is established by a third party (trusted by all the communicating

parties) to assert the claimed identity of the individuals to each other. This third party is often an official trusted entity within that domain, e.g. an organizational body for doctors certifying a person's claim of being a doctor or the government of a country certifying the citizenship claim of a person.

In the real-world identification, the trusted third party issues paper-based credentials to certify the claim of a person. They allow the linkage of attributes to a person and enable identification and identity authentication in a single stand-alone document [17]. Different paper-based credentials are used depending on the domain. This includes an ID card or certificate in the case of the organization body of doctors or ID cards and most especially passports issued by the government for certifying a citizen's claim as identified above. Other official paper-based identity documents may also include a driver's license or birth certificate. These identity documents strongly assert the verifiable identity of the carrier of the document.

Today, the most popular identification credential in the physical world is the Passport. The application of Passports is suitably described by Camp [17] as, "identification ('I am me') and identity authentication ('my government authenticates that I am me.')". It links attribute authentication (citizenship) with identity authentication (name, photograph and data) to enable off-line identification [17].

In [25], physical world identity verification is considered to be a relatively straightforward task, in which identifying persons present themselves physically to the entity requiring proof of identity, along with a set of government generated credentials, such as a Passport, ID card or driver's license. This by default involves, given a set of person attribute data (e.g. photo, name, age etc.), another entity is able to verify and confirm that the person making the claim is indeed the person to whom the attribute data belongs. Depending on the result of the identity verification process, access to the requested service/transaction is either granted/completed or denied/canceled.

On the other hand, anonymity in the real world is provided by documents that do not include any PII such as a ticket to a movie, cash etc. In both cases, only the authenticity of the document is verified; it does not require its carrier to be authenticated before it could be used or spent. Pseudonymous documents for example include a subscription bus ticket, do not carry any PII, but include a unique constant identifier e.g. serial number, which could form a basis to identify the holder in combination with other data.

2.3. Digital identity

A digital or electronic identity in the context of this thesis is simply defined as an identity used by a person on the Internet. It is an identity presented by a person on the Internet to make him/herself known to service requesting to know who he/she is.

The Internet by design is anonymous in nature, with everyone being able to access everything and anything. However, the proliferation and adoption of more (and high risk/value) services on the Internet, have given rise to the need to limit access to only a set of known, registered and authorized persons. This has led to a multiplication of identities, not all of which are the same, and/or reflect a person's 'real' identity [25]. All the different forms of identities used on the Internet today can be classified into two primary groups, both described as follows.

Self-asserted identity: This refers to identities that are based on self-defined person attributes. Users normally sign up or register to a service using self-asserted attributes, including name, date of birth, location information, email address etc., and create credentials (username + password), with which they would authenticate to the service thereafter. Typically, a person may choose to protect his/her personal information by using pseudonyms to access services that do not require real world identities. This type of identity may be sufficient for webmail, social networks, news sites, eCommerce accounts etc. However, online banking and government services for example require a different form of identity, one with more trust due to the high valued nature of the services [25].

Official digital identity: This refers to identities rooted in real world official identity documents. In applications ranging from online banking, to electronic tax filing, to controlling entry to secured office buildings, to ensuring payment, the need for a verified identity is more important than ever [24]. They make use of credentials derived from strong registration processes that traverse the physical and online worlds [25]. To acquire an official digital identity credential, people are required to present a real-world official identity document such as birth certificate, passport etc. to authenticate their identity before being issued with identity credentials used online. The digital identity credential is then used by the entity to authenticate a claimed identity. A service provider validates the credential to obtain a level of confidence in the identity claim [24].

Today, the Internet has been highly commercialized that everything a person does on the Internet could constitute a revenue generation opportunity for different applications, especially for advertising. Thus, there have been an increasing demand by service providers like Google, Facebook among others for real identity on their platforms even when Pseudonymous identities should be sufficient. The capture, processing and use of personal information and, in many cases, personally identifiable information by the various online platforms, means we are gradually seeing the erosion of control over the disclosure of our digital identity and the ability to remain anonymous on the Internet [24].

2.4. Levels of Assurance (LoA)

The Level of Assurance (LoA) in an asserted identity could be defined simply as the degree of confidence reached in the identity authentication process that an entity is indeed who it claims to be. The primary standard definition of the Level of assurance in an asserted identity (or authentication solution/credential) is according to the ISO/IEC 2915 standard [15]. The ISO/IEC 2915 defines four levels of assurance, which today form the basis of many assurance frameworks used internationally. Each of the levels defines the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity claiming a particular identity (i.e., the entity) is in fact the entity to which that identity was assigned [15].

In Europe, under the EU's eIDAS definition [8], three levels of identity assurance are defined. The three levels Low, Substantial, and High corresponds to Levels 2, 3 and 4 of the ISO/IEC 2915 definitions respectively. According to its definition, Levels of Assurance characterize the degree of confidence in the electronic identification credential used in establishing the identity of a person, providing assurance that the person claiming an identity is in fact the person to which the identity was assigned.

Normally, a service provider determines the minimum level of assurance for identification on its service and requests for an identification credential that corresponds to the required LoA. The identification credential, in return, indicates to the service provider how much trust could be placed in the returned information or signature. For example, a service provider requiring a lower LoA (e.g. LoA1), may only require the correct entry of a shared secret (e.g. password) for successful identification, while identification at higher LoAs may involve using a cryptographic based challenge-response credential, as well as a number of different authentication factors.

The assurance level for a particular identification credential depends on the degree of confidence it provides in the claimed or asserted identity. The trust or confidence is derived from:

- The strength of the entity registration process, for example, identity proofing, verification, and authentication. Otherwise referred to as identity assurance,
- The strength of credential issuance and management processes including for example, the entity issuing the credential and the procedure it follows to issue the credential, and
- The strength of the authentication method. Otherwise referred to as authentication assurance.

Both the ISO/IEC 2915 and the EU's eIDAS regulation define minimum requirements and technical specifications for the assurance levels defined. In the case of the eIDAS regulation, the specifications and requirements are set out in the accompanying EU regulation 2015/1502 of 8 September 2015.

According to both definitions, the LoA is determined based on the risk involved in the identification of an entity and the amount of loss that could result from an erroneous identification. Thus, the higher the risk or value of the transaction, the higher the required level of assurance. The remaining part of this section describes the different levels following the ISO/IEC 2915 and eIDAS definitions.

Figure 1 below shows the characterization of the LoAs according to [3].

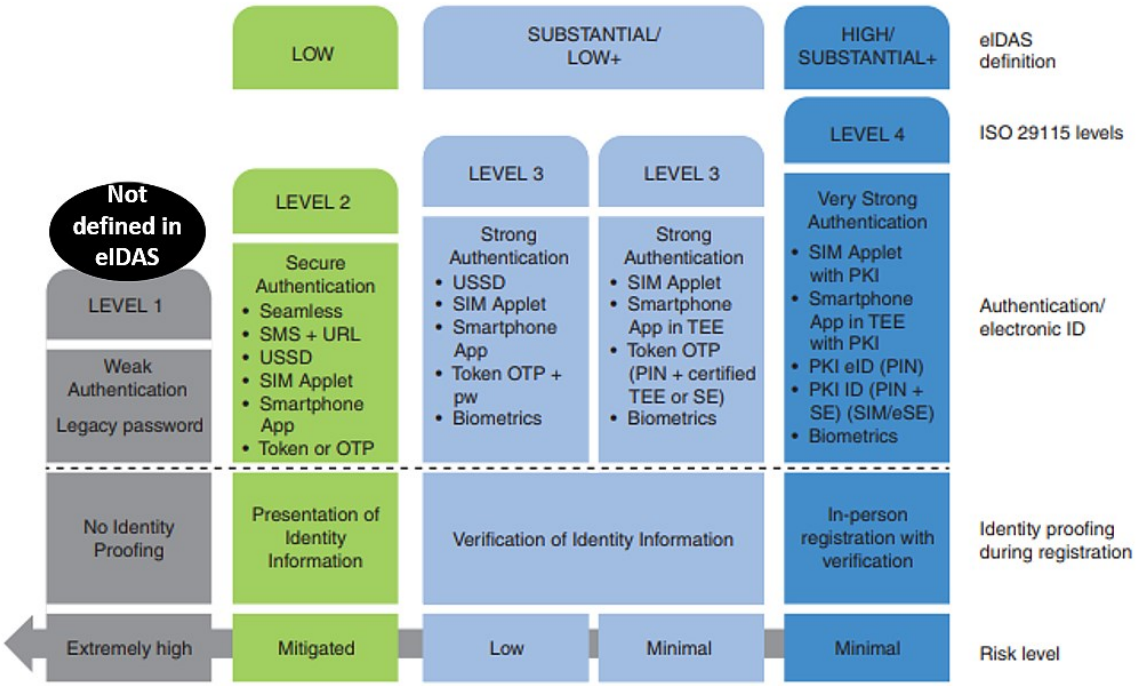

Figure 1: Levels of Assurance definitions [3]

Level of Assurance 1 (LoA1)

At LoA1, there is minimal (i.e. little or no) confidence in the asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events. There is no identity proofing requirement at level 1. LoA1 allows a wide range of credentials to be used including password challenge-response for authenticating identity. Successful LoA1 authentication requires that the person prove that he/she is in control of the authentication credential (e.g. password). For LoA1, implementing complex communication protection mechanisms is not mandatory but transmitting credentials in plain text is not recommended.

Level of Assurance 2 (LoA2)

At LoA2, there is some confidence in the asserted identity of the entity. LoA2 is used when a moderate risk is associated with erroneous authentication. It is equivalent to ***Low LoA*** according to the eIDAS definition, which refers to an electronic identification credential that provides a limited degree of confidence in the claimed or asserted identity of a person.

Some form of Identity proofing is introduced at LoA2, requiring presentation of identifying information from an authoritative source during registration. Authentication in LoA2 uses a single factor that could be a password or PIN. Successful LoA2 authentication requires that the person prove that he/she is in control of the authentication credential. It is recommended that eavesdropping, replay attacks etc. be suitably prevented.

Level of Assurance 3 (LoA3)

At LoA3, there is high confidence in the asserted identity of an entity. It is equivalent to ***Substantial LoA*** according to the eIDAS definition, which refers to an electronic identification credential that provides a substantial degree of confidence in the claimed or asserted identity of a person.

LoA3 provides a high confidence that the user claiming an identity is the same entity to which the identity was assigned, proved though the use of a multi-factor authentication e.g. a mobile phone or OTP token and PIN or biometric e.g. fingerprint etc. LoA3 is used where a substantial risk is associated with erroneous authentication. Identity proofing procedures (either face-to-face or remote) require presentation of identifying information from an authoritative source to support the claim of identity during identity registration and verification done by the registration authority.

Successful LoA3 authentication is mostly based on the possession of a cryptographic credential. Examples of accepted credential include soft cryptographic tokens, hard or device tokens etc. Sufficient cryptographic mechanisms must be implemented to protect the complete authentication infrastructure from compromise including eavesdropping, replay, man-in-the-middle attacks etc.

Level of Assurance 4 (LoA4)

LoA4 represents the highest level of assurance defined by the ISO/IEC 2915 standard. At LoA4, there is very high confidence in the asserted identity of an entity. It is used when a high risk is associated with erroneous authentication. It is equivalent to ***High LoA*** according to the eIDAS definition, which refers to an electronic identification credential that provides a higher degree of confidence in the claimed or asserted identity of a person than what is obtained in substantial assurance level.

LoA4 is similar to LoA3, but it adds the requirements of in-person identity proofing at a Registration authority and verification of information using official government sources and documents. LoA4 also mandates the use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys.

LoA4 authentication requires the use of multi-factor authentication for accessing the private data/keys stored on the tamper-resistant hardware token. It also defines that the storage and transmission of PII and other sensitive data must be cryptographically protected and safe from attacks such as eavesdropping, replay, man-in-the-middle attacks etc.

2.5. Authentication

Authentication simply refers to the process of proving that the identity of an entity is as claimed. According to [15], the authentication process involves the use of a protocol to demonstrate the possession and/or control of a credential in order to establish confidence in the identity claim. The protocol requirements and authentication procedure depend on the applicable or expected level of assurance in the identity claim. A username, data attribute, unique identifier or PKI certificates represent identity, while the possession of a password, PIN, biometric data, etc. assure the service provider requesting identification that the user is who she claims to be.

2.5.1. Factors

According to Wikipedia,[8] authentication factor refers to the way or process used to authenticate or verify the identity of an entity. Not all authentication factors provide the same strength, and a combination of factors is used to increase assurance.

- Knowledge - simply put as *something you know,* - it is the most common factor on the Internet today. Examples are password and a PIN (personal identification number).
- Possession - simply put as *something you have,* - Demand for this factor in addition to knowledge factor is increasingly common today for two/multi-factor authentication. Examples include a person's mobile phone, computer, smartcard, OTP (One-time password) token, TAN (Transaction authentication number) list, key card, among others.
- Inherence - simply put as *something you are,* - commonly used for what is called biometric authentication. There has been an explosion of the usage of biometrics for authentication in recent times, with most common application found in smartphone authentication. Application on the Internet is gradually rising, e.g. for authorizing payment on Apps such as Apple Pay etc. Most common biometrics used are fingerprint scanning (e.g. Apple/Android TouchID), or facial recognition (e.g. Apple faceID), Iris scanning, voice recognition etc.
- There is also a fourth, but not widely used factor "Behavior" - simply put as *something you do*. It includes patterns of behavior such as typing patterns, geo-location etc. It hasn't seen many applications on the Internet.

Figure 2 shows a characterization of the various authentication factors discussed above according to [3]

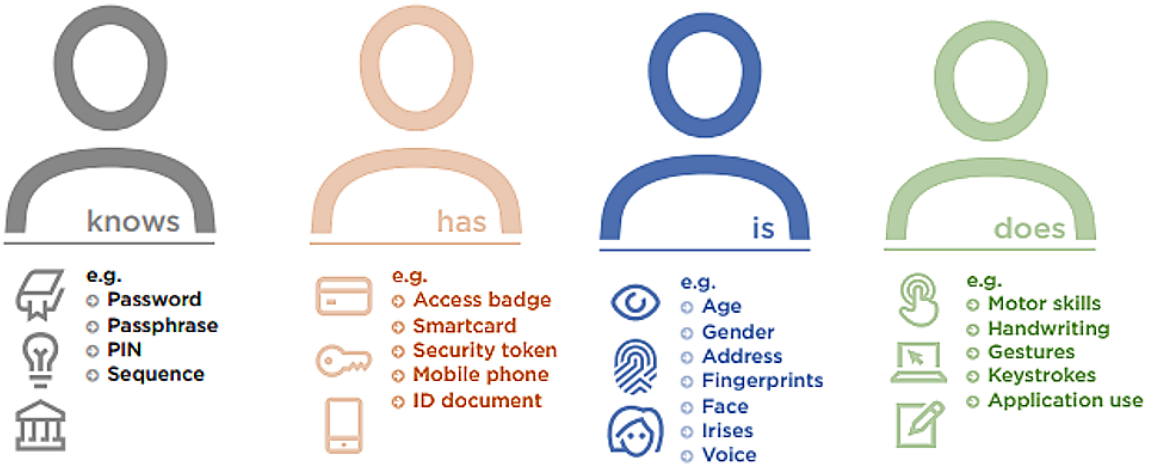

Figure 2: Authentication Factors [3]

Authentication on the Internet today in its most basic form, uses a single factor, e.g. username and password combination. This is sufficient only for LoA1 authentication. Higher LoA (i.e. starting from LoA2) authentication must make use of at least two or more authentication

[8] *Authentication.* Wikipedia. Retrieved from: https://en.wikipedia.org/wiki/Authentication (04/04/2018)

factors. This is referred to as two or multi-factor authentication. For example, using a smartcard (something you have) and a PIN (something you know). The use of two or more elements from the same factor group (e.g. Password and PIN) for authentication does not constitute two/multi-factor authentication.

2.5.2. Implementation methods

The following are some of the technologies used for implementing authentication on the Internet today.

Passwords: Password-based solutions allow users to identify and authenticate to a service by entering their username and password. The passwords could be static (one password for every login) or dynamic (e.g. One Time Passwords) [21]. Passwords is the oldest and still the most popular authentication method used on the Internet today.

Biometrics: Biometrics based solutions allow users to identify and authenticate to a service on the Internet using their inherence factors. These factors include physical features such as a photograph of a person's face, his/her fingerprints, hand, Iris, ear patterns etc. or behavior factors such as voice, hard writing, among others.

Symmetric key cryptography: Also referred to as secret-key cryptography, makes use of a symmetric cipher in which the same key is used for encryption and decryption. As only the communicating parties know the shared key, the parties can be relatively assured of the identity of the person they are communicating with. A one-to-one symmetric key is often used today on the Internet to secure communication between a server and a client. Thus, the server trusts that anyone possessing the key is the intended party to whom the communication is intended. A popular example of an electronic identification solution based on symmetric key cryptography is GSMA's Mobile Connect solution.

Public Key Cryptography (PKC): Also referred to as Asymmetric key cryptography, it makes use of a pair of related keys, private and public for encryption and decryption [18]. The private key remains concealed by the key owner, while the public key is made available publicly. Although, the public key is available publicly, it is computationally infeasible to guess or generate the private key from knowing only the public key. The most popular application of PKC today is in public key infrastructure which is the foundational technology for most strong electronic identity solutions.

2.6. Public Key Infrastructure (PKI)

According to Wikipedia,[9] "A public key infrastructure (PKI) is a set of roles, policies, and procedures used to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption on the Internet". It refers to a technology which is based on Asymmetric or Public key cryptography, which involves the use of two different keys for

[9] Wikipedia. "*Public Key Infrastructure.*" Retrieved from: https://en.wikipedia.org/wiki/Public_key_infrastructure. (Accessed 26/04/2018)

encrypting and decrypting data; one which is publicly-made available ("public key") and another, which is kept secret ("private key"). A public key is linked to the identity of a person through a digital certificate issued by a trusted third party referred to as a Certification Authority.

Today, PKI forms the foundation of security on the Internet, defining the policies and procedures that make the use of public key cryptography possible on the Internet. Most common applications of PKI in daily life on the Internet include on Internet browsers, using TLS (Transport Layer Security) to guarantee end-to-end security when accessing web pages, S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy) standards for email. Other applications include electronic identity implementations found in national e-ID cards, Mobile PKI, electronic chips in passports, payment cards, among others. PKI, when used for implementing electronic identity schemes provides a solution that offers the highest levels of assurance in a digital identity comparable to what could be obtained from an official paper-based identity document.

The PKI role that assures valid and correct registration of a person's identity is called a **Registration Authority (RA)**. The RA is responsible for accepting requests for digital certificates and authenticating the entity making the request. It is a trusted actor that establishes, verifies and vouches for the identity of a person to the certificate issuing authority. It performs entity identity authentication, verification and proofing according to a specified procedure, typically evaluating an official identity document (e.g., passport, national identity card, a driver's license etc.) and/or verifying the claimed identity from records in official databases [15].

The RA could either be an integral part of the Certificate Authority or external to it and trusted by the CA to execute the processes related to the enrolment and registration of entities in a way specified or approved by the CA. It is also responsible for binding the key to the person, which depending on the level of assurance, could be done by software or under human supervision.[10] The combination of strong registration and certification expressly asserts that the person who uses the private key is whom he/she claims to be.

Figure 3 shows a high-level presentation of the Public Key Infrastructure and the interactions between the primary stakeholders in the infrastructure.

[10] *Public Key Infrastructure.* Wikipedia.

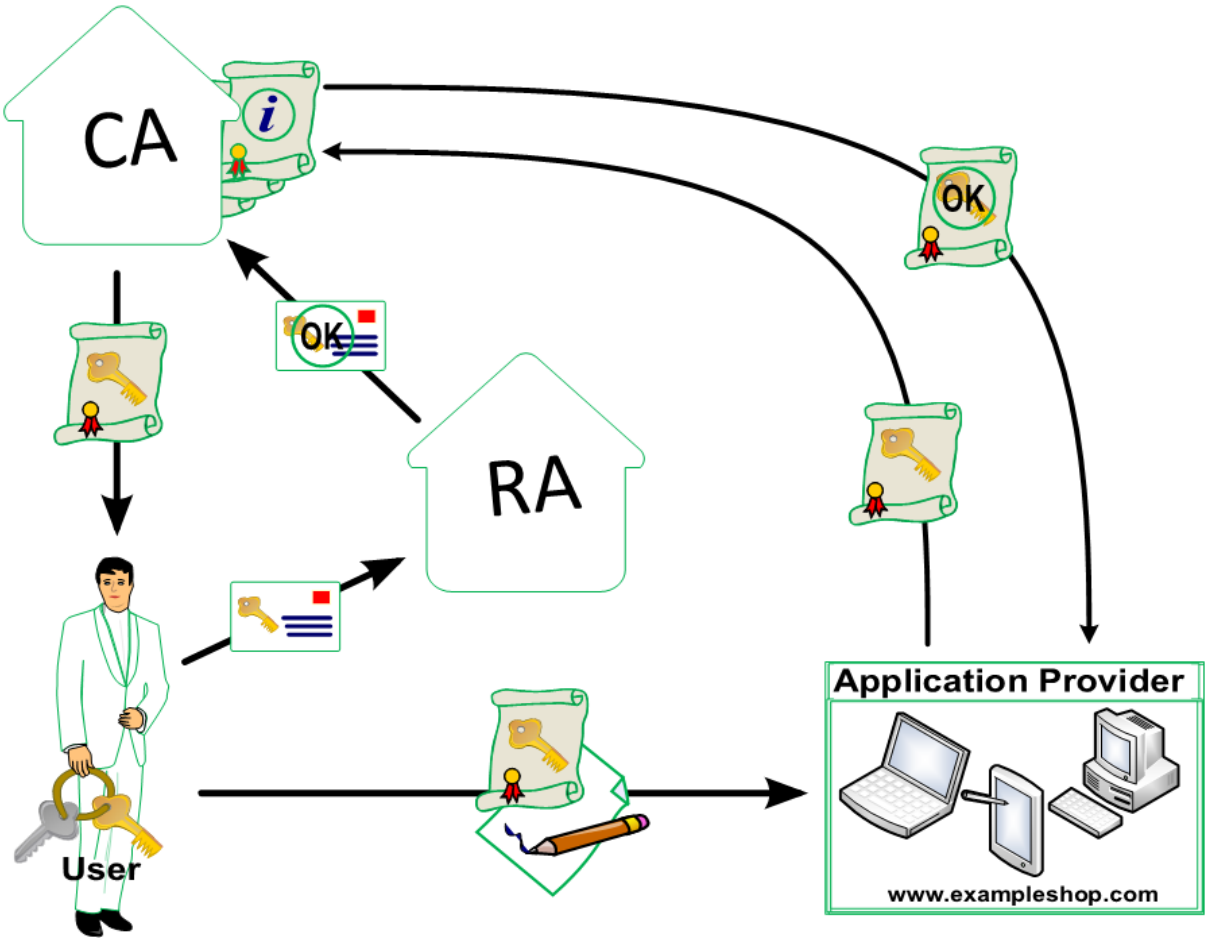

Figure 3: Public Key Infrastructure[11]

Certificate Authority: The certificate Authority is the trusted PKI role responsible for certifying the identity of an entity through the issuance of a digital certificate. A *digital certificate* is a document that associate a public key with an entity using a digital signature. The CA uses its private key to sign the public key of the entity, creating a digital certificate which gives legitimacy to the claimed identity of the entity. It certifies the ownership of a public key (and in return the electronic identity) by the named subject of the certificate [23]. The accepted certificate standard on the Internet today is the X.509 Version 3.0 certificate, defined in RFC 5280 [31]. It defines what goes into a Public key certificate, as well as CRL information of the certificate. This includes a unique certificate identifier, PII of the subject, certificate validity, issuer information, signature algorithm, the public key, among other information.

Two documents, namely a *Certificate Policy (CP)* and *Certificate Practice Statement (CPS),* are used for addressing the intended use of issued certificates and operating procedures of the CA and/or the complete public key infrastructure. The CP allows third parties to analyze the PKI's procedures and respective trustworthiness, while the CPS gives a detailed description of

[11] *Public Key Infrastructure.* Wikipedia.

the practices followed by a CA in issuing and managing certificates [20]. RFC 3647 [32] defines the guidelines for writing the CP and CPS documents.

The basic premise of PKI is the high level of confidence in the public key it certifies. It provides a provable binding of a public key with its associated private key [22]. The digital certificate serves as the basis for the authentication of the subject it identifies. An authentication factor, (discussed in section 2.5.1 above), is used to prove possession and ownership of the certificate during an authentication. The successful authentication of the certificate owner (subject) produces a *digital signature.* According to [19], "Digital signatures create persistent, tamper resistant evidence of 'who did what to whom', binding a real entity or person to a transaction". Common digital signature algorithms in PKI are RSA and ECDSA. A valid digital signature provides authentication, non-repudiation and integrity of communication and messages exchanged between parties in the communication. With built-in support for data origin authentication and nonrepudiation, public key infrastructure, offers a strong assured solution for person identification on the Internet.

2.6.1. Common standards and protocols in PKI

This section describes some of the most important Public key cryptography standards (PKCS) and protocols, found in the solutions surveyed in this thesis.

PKCS is a group of standards for public-key cryptography created by RSA Security to boost the popularity and usage of public key cryptography on the Internet.[12] Today, international bodies such as IETF, ISO/IEC, ITU-T, among others, maintain most of the PKC standards. In addition to PKCS, some of the most important PKI standards and protocols, such as X.509, CMP, OCSP etc., are also described.

The standards and protocols covered below do not constitute an exhaustive list as there are many more PKC/PKI standards and protocols that we are unable to cover.

PKCS#1 RSA Cryptography Standard is the first PKCS published by RSA Laboratories. RSA is a public-key algorithm invented by Rivest, Shamir, and Adleman in 1978. The PKCS#1 standard provides definitions and recommendations for implementing the RSA algorithm for public-key cryptography. It defines the mathematical properties of keys, cryptographic primitive operations, signature and encryption schemes and related ASN.1 syntax or representing keys and for identifying the schemes. The current version of the standard is PKCS#1 v2.2, defined in RFC 8017 [33].

PKCS#7 Cryptographic Message Syntax Standard defines a generic syntax for different forms of cryptographic content, including, data, signed data, enveloped data, signed and enveloped data, digested data, and encrypted data. It defines the syntax used to digitally sign, digest, authenticate, or encrypt arbitrary message content. RFC 5652 [34], defines the latest version of CMS.

[12] Wikipedia. "*PKCS.*" Retrieved from: https://en.wikipedia.org/wiki/PKCS (Accessed 23/04/2018)

PKCS#10 Certification Request Syntax Standard defines a syntax for requesting certificates from a certificate authority. Referred to as a Certificate Signing Request (CSR), it consists of the public key for which a certificate is to be issued, information about the subject and optionally a set of attributes, signed with the private key of the subject. The CSR is sent to the CA, who having validated the request, issues an X.509 certificate for the public key. The current version of the standard is PKCS#10 v1.7, defined in RFC 2986 [35].

PKCS#12 Personal Information Exchange Syntax Standard, describes a file format for transfer and storage of cryptographic data. It defines a syntax for bundling personal identity information, such as private keys, certificates, etc. as a single file, allowing a person to easily import and export the data. The current version of the standard is PKCS#12 v1.1, defined in RFC 7292 [40].

PKCS#13 was originally reserved for Elliptic Curve Cryptography (ECC) but has not yet been published in mid-2018. It is meant to define a standard for ECC, analogous to PKCS#1. Today, ECC is gradually seeing more adoption on the Internet as an alternative to RSA because it requires smaller key sizes while not losing any of the security and key strength expected from a comparable RSA key size (e.g. ECDSA with a 256-bit curve comparable in strength to RSA key of 2048-bit size).

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, defines a standard format for public key certificates and Certificate Revocation Lists (CRLs). It was defined by ITU-T, and the current version of the standard is X.509v3. An X.509v3 certificate contains a distinguished name (which among other information contains the certificate serial number and subject PII) and public key, certificate validity, issuer information, and signature algorithm. The X.509 standard specifies certificate revocation lists (CRL) as a way to distribute information about invalid certificates, as well as path for validating certificates in the trust chain. The standard also includes standardized extensions which allows individual PKI implementation to define own extensions such as key usage (for defining the certificate use cases), certificate policies etc. [20]. RFC 5280 [31], defines the current version of the standard.

Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) is another important PKI standard, which defines protocol messages for X.509v3 certificate creation and management. It enables interactions between PKI components, including messages used for CA - client integration, initial certificate creation, lifecycle management such as key/certificate updates, recovery, revocation, etc. [20]. RFC 4210 [36], defines the current version of the standard.

Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) is an accompanying message format used with CMP. It defines the message format used to convey a certificate signing request to a CA to issue an X.509v3 certificate for an entity. The certificate request message includes a certificate signing request (containing the public key and subject info), a non-mandatory proof of possession (used to ascertain subject is in possession of the private key corresponding to the public key to be certified) and other optional

information fields communicated to the CA using CMP. RFC 4211 [37], defines the current version of the standard.

X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP), specifies a protocol alternative to CRL for determining the status of an X.509v3 certificate. OCSP allows a client to query an OCSP responder to check the revocation status of an entity's certificate without recourse to CRLs. It specifies the request and response formats for OCSP queries. RFC 6960 [38], defines the current version of the standard.

Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), specified in RFC 3161, defines a protocol to achieve a proof of timeliness and guarantee the long-term validity of digital signatures [39]. With the increasingly important use of digital signatures, timestamping is used to increase the non-repudiation features of a digital signature. A time stamp on a signed message could be used to proof that the message was signed prior to the date of expiry or revocation of the key used to sign the message [20].

2.6.2. Strong electronic identity lifecycle

A strong electronic identity solution must provide authentication of identity, integrity of authenticated identity and most importantly the non-repudiation of the claimed identity. It must be based on an official identity enabling the linkage of the physical world identity of the person to his/her digital identity.

This require that the electronic identity creation process follow clear non-repudiable steps such that the required level of trust could be achieved. Figure 4 highlights some of the important processes and steps carried out when creating a strong electronic identity as described in this section [3], [23].

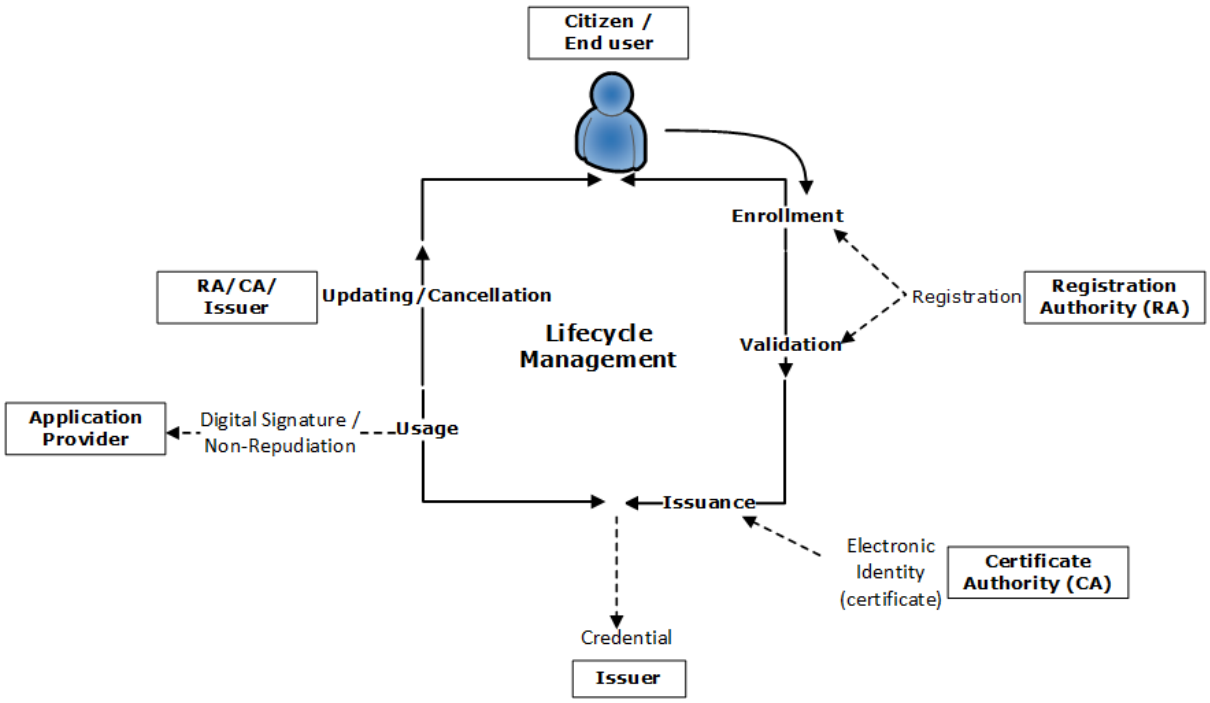

Figure 4: Strong electronic identity Lifecycle [3]

Registration: The registration stage is the first step an entity goes through towards acquiring a strong electronic identity. The process begins when the entity visits a Registration Authority (RA) to request for the issuance of a certificate for his/her claimed identity. The RA verifies the authenticity of the identity and credentials, and thereafter forwards the certificate signing request to the CA on behalf of the entity, when the entity has been appropriately registered. Depending on the Certificate Practice Statement, Certificate Policy and privileges associated with the requested certificate, the identity verification may require a physical appearance and/or submission of appropriate official identity document.

Issuance: The certificate issuance stage comprises of a number of steps including:

Credential Initialization and Key Pair Generation: Upon successful verification of the entity's identity by the RA, one or more PKI key pairs are generated for the entity, using well-established algorithms such as RSA or ECC. The key pair generation process could either be initiated by the issuer (e.g. in physical e-ID card implementations), who then initializes the card for the entity during the registration, or by the user in onboard key generation (e.g. in mobile PKI implementations).

Certificate Creation: After the entity credentials have been initialized and key pairs generated, the RA sends a certificate signing request containing all the required parameters to the Certificate Authority for certificate issuance. The CA issues an X.509v3 certificate to the entity that binds the entity (subject and public key) to a particular private key.

Usage: At this stage of the strong e-ID lifecycle, the entity to which the certificate was issued is able to use the certificate to proof (or authenticate) his/her identity online. This process involves also *certificate validation*, which is performed to ascertain the integrity and validity (whether expired/revoked) of the certificate before its usage is accepted [23]. Certificate usage cases are discussed in section 2.7, the use cases fall under the following groups:

1. *Authentication* – to establish the claim of an identity as true.
2. *Non-repudiation and Message Integrity* - digital signatures in the messages ensure that exchanged messages between communicating parties are in their true form on delivery and that the parties could not later repudiate a message as originating from them.

During the lifetime of the certificate, there might be need for ***key pair or certificate update***. For example, as the certificate closes in on expiry, it may be refreshed (i.e. auto renewed before expiry), provided the keys are still valid and remain uncompromised [23].

Revocation/Cancellation: A certificate may become invalid for two main reasons, (1) if the certificate is not within validity period (i.e. the certificate has expired or has not yet entered use), and (2), if certificate is revoked by the issuing CA. Case 2 may be as a result of the keys becoming compromised [23]. The CA notifies the revocation status of a certificate through a CRL or using OCSP. The revocation of the certificate may necessitate a key renewal process where new keys are generated and a new certificate is issued, or a complete ***Deletion*** which involves the removal of the subject account and data from the public key infrastructure.

2.7. Uses of strong electronic identity

Applications of strong electronic identity can be found today in almost every industry where security, privacy, identity assurance, non-repudiation etc. are important. The use cases range from simple authentication, to message integrity and non-repudiation. The following briefly looks at some of the use cases from a few identified environments.

Citizen to government

An important requirement to access government services is strong authentication of the citizen. Strong e-ID solutions such as smartcard-based e-ID cards, Mobile PKI, BankID, etc. allow citizens to be reliably authenticated to government applications, removing the need to physically appear at an office and reducing costs on the government side. Below are example use cases in citizen to government interactions.

e-Taxation: In most countries today, citizens file their tax forms on paper which often takes a couple of days to complete the process. A citizen with a strong e-ID credential could quite easily authenticate to an e-tax system and complete the same operation in only a matter of minutes. This saves both the citizen and the government time and resources that would have been expended handling paper. Today filing taxes online is an important application of strong e-ID in countries such as Finland, Estonia, and Norway.

e-Health: In countries where digitized medical records are available, authentication using strong e-ID solutions allows citizens to access their medical data and related information (such as recent appointments, prescriptions, reports etc.). Citizens could also book appointments with doctors online, deliver patient information to the booked doctor and enables the doctor to access the citizen's medical history as required.

e-Voting: Electronic voting is another citizen to government application of strong e-ID. It offers a convenient alternative to the casting of paper ballot. The e-ID credential allows citizens to strongly authenticate to the e-voting system and cast their votes remotely without visiting a physical polling center.

e-Education: Like other public eservices, strong electronic identity is critical to enable access to educational platforms by students, teachers, parents and guardians alike. e-Education provides students, teachers the ability to learn and deliver education from anywhere and at any time. It also allows parents and guardians access confidential educational records and track the development of their children or wards. e-Education with strong electronic identity provides an opportunity for government to direct the way public education is provided to meet the needs of students and teachers in the 21st century.

Citizen services, citizen information update: Citizens could strongly authenticate to government social services including social security and welfare systems, pension systems, apply for benefits and other entitlements etc. Citizens could also securely report information updates e.g. a change in address, to government databases quickly; notify the government of change in circumstances (e.g. loss of job) among others.

Customer to Business

Like in citizen to government, strong e-ID provide ways for customers to enter relationships with companies and transact with them remotely without the need to appear physically at the business offices. Below are typical use cases.

Customer registration and logins: It has been widely reported that many customers drop out of a service at the point of registration. Strong e-ID allows customers to reliably sign up to a service without needing to fill complicated forms.

Strong e-ID also provides secure and reliable logins to online service provider platforms, ranging from social media, ecommerce platforms etc. Strong e-ID, in addition to providing the highest levels of assurance (i.e. LoA4) authentication, could also be used to authenticate to online applications requiring lower levels of assurance (e.g. LoA2), pseudonymous logins or even anonymous authentications such as age verification etc.

Online banking: Online banking constitutes probably the biggest application area of strong e-ID in customer to business relations. To combat fraud and money laundering, governments across the world have placed strict requirements on financial institutions to know their customers. Strong e-ID offers two important use cases in banking as listed below:

1. New Customer enrolment (i.e. opening a bank account), and
2. Performing a transaction (e.g. transferring money or obtaining an account statement).

Banks must comply with customer due diligence standards, which means that they are obliged to identify and know their customers before doing financial business with them. Today, opening a bank account has one key requirement: Know your customer (KYC) [6]. Traditionally, a client looking to open an account with a bank must go to the bank's offices and present an identification document so that their identity could be ascertained and verified. A strong e-ID removes the need to visit the bank's offices and thus, facilitates online banking. A strong e-ID solution such as Mobile PKI or national e-ID card delivers official and verified personal information about the prospective customer to the bank allowing the bank to easily meet the KYC requirements [30].

In addition, with the increasing rise in cases of banking fraud, it has become a requirement for banks to implement strong identification systems for customer authentication to their online banking platforms and ensure non-repudiation of transactions. Strong e-ID such as those reviewed in this thesis, implement multi-factor and/or tamper-resistant systems for customer authentication and digital signatures for non-repudiable transactions.

Business to Business (B2B) and Business to Government (B2G)

B2B and B2G, for example account for the biggest push for the European drive for a single identity market. It is meant to cut red tape and make it easier for enterprises to do business both locally and across borders. It reduces bureaucracy in allowing companies to be registered faster digitally and contracts to be completed completely online [21]. The biggest advantage of strong e-ID is doing away with paperwork and bureaucracy in a B2B and B2G relations.

For example, submission of VAT or income tax return, account for some of the most bureaucratic government services in most countries. For many enterprises, filing taxes on paper makes the process long and complicated. Strong e-ID for enterprise personnel or the enterprise itself (so called e-seals) allows non-person entities (or their employees) to easily access services such as tax reporting, business registration, importation/exportation of goods etc.

e-ID implementations for organizations referred to as eSeals in the eIDAS regulation can also be used to digitally sign contracts and electronically stamp documents, on behalf of the organization.

Employee to Business

In employee to business relationships, strong e-ID enable employees to reliably authenticate to company's infrastructure, including authentication for remote work or authentication to access company building, etc.

Other Use Cases

Other use cases exist that extend beyond the limited use case/scenario groupings given above. In theory, strong e-ID could also be used to prove entitlement to services offline, including usage as transport tickets, or as a key token to physically gain access to libraries and other public spaces etc. Also, strong e-IDs could also be integrated with email clients to provide end-to-end S/MIME e-mail encryption and digital signing.

Other applications such as e-Residency as seen in Estonia allow non-citizens outside the country to establish and manage business in Estonia and the EU completely online from anywhere in the world. Entities under the e-Residency program could apply for a bank account, digitally sign and transmit documents, declare taxes online etc. as part of the scheme.

Chapter 3

Physical e-ID cards

Unarguably, the best source of identification for people is the government and in most countries around the world where strong electronic identity has been introduced, physical e-ID cards have been the go-to solution for implementation. In most countries across the world, government issued identity documents are considered as the standard for citizen identification and authentication by service providers. The government is considered a natural and irrefutable source of identity for the citizens as it issues birth certificates which often form the basis of the information about a particular citizen containing details such as name(s), date of birth, nationality etc. [46].

Traditionally, citizen identification has mostly been provided by the government in the form of physical ID cards and Passports. With the move of most of the services from primary offline services to eservices, the demand for the identity documents usable online became apparent. Today, other identity solutions acquire their validity by being rooted/based on government issued identity documents. Therefore, the government is in the best position to validate the identity of its citizens online. To be able to meet this demand, many governments moved to begin issuing identity cards that could also be used for online identification and authentication [4], [14].

The main driver of government interest in electronic identity was an interest in moving closer to the citizens through the provision of government services online (e-Gov). The government needs to identify the citizens for its own services including e-health, taxation and benefits. Government agencies already have a trench of data about its citizens stored in databases and electronic identification could be built on the existing infrastructure [4].

Smartcard chips embedded in the national identification cards appear to be the favored solution when countries look to implement electronic identity solution. The implementation of a government issued e-ID solution was started by the Finnish government when it issued the FINEID in 1999 as the world's first smartcard based National e-ID card [4], [5], which have since been followed by many more countries [46].[13] The relatively matured smartcard technology meant the cards could provide a *"dual"* functionality as being usable both for online and offline authentication. For online authentication, this is a natural choice because the

[13] *Electronic identification.* Wikipedia.

tamper-resistant chip and cryptographically signed information increase the difficulty of copying and falsifying identity cards. Moreover, the card (possession) and PIN code (knowledge) provide two-factor authentication in one physical package. Similarly, user details such as photo, name, identification number, date of birth, nationality etc., can be printed on the card surface allowing the card to be usable for physical identification [4].

The National e-ID card offers a hardware-based solution for IDs and digital signatures, employing smartcards issued by the government as a secure element to offer unique identification of citizens online. The typical electronic identity card has the format of a regular bank card, with printed identity information on the surface, such as personal details and a photograph, as well as an embedded microchip [14].

The government is normally responsible for manufacturing the cards (or acquiring them from a smartcard vendor), creating the keys, issuing and storing the certificates. Also, the services related to blocked-card registers and time stamps and the distribution of the cards would belong to its responsibility. The embedded microchip stores subject details, as well as Public Key Infrastructure (PKI) data about a specific person to whom the card is issued, supported by a National PKI system comprising of all the needed components/entities and roles. Today, the cards normally include two digital certificates, one for authentication and the other for signing. Information in the card is protected by a PIN code [5], [28], [42], [46].

Normally, acquiring the card requires that the citizen be first authenticated physically e.g. visiting a designated government Registration Agent (RA) such as the Police or post office where the applicant's personal details are collected, and his/her identity is verified. To use a card, the user must have a card reader and a personal PIN-code for the card.

3.1. Technical features

A smartcard is often a plastic card (similar in shape and size to a bank card) that contains an embedded computing chip. As a card material, Polycarbonate (PC) is often preferred. It is a thermoplastic polymer with excellent toughness characteristics. The computing chip is under a gold contact pad on the surface of the card [14]. The figure below shows a high-level view of a typical smartcard.

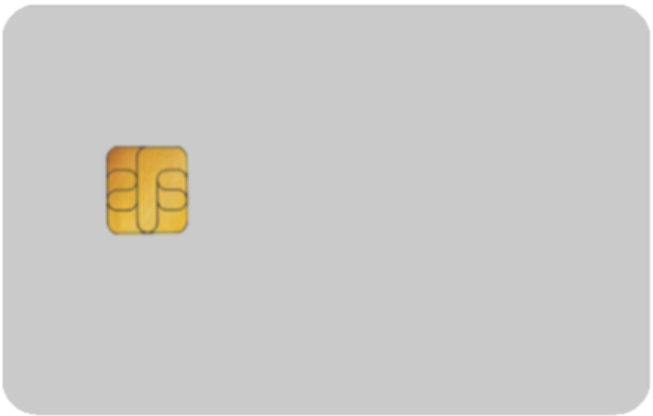

Figure 5: Contact e-ID card schematic

The ISO/IEC 7816 standard specifies an accurate card size, chip location, card material and optional parts like magnetic stripe or photo etc. [14], [29]. The communication between a card and an application usually takes place via a card reader using either electrical contacts (as defined in ISO/IEC 7816) or a contactless radio frequency (RF) interface (e.g. defined in ISO/IEC 14443).

The integrated Circuit chip in a smartcard makes it possible to use the card for complex operations including the storage and processing of sensitive information. One of the most important applications of the card is the general identification of the cardholder.

The smartcard chip is a prime example of a qualified electronic signature creation device, as defined in Annex II of the EU eIDAS regulation [8]. It provides a tamper-resistant environment for storing security-sensitive information e.g. cryptographic credentials.

3.1.1. Components

A smartcard is typically a small conventional computer containing various internal components that allow it to hold keys and carry out complex operations required to securely identify and authenticate the holder. The key components include the following as shown in *Figure 6* below.

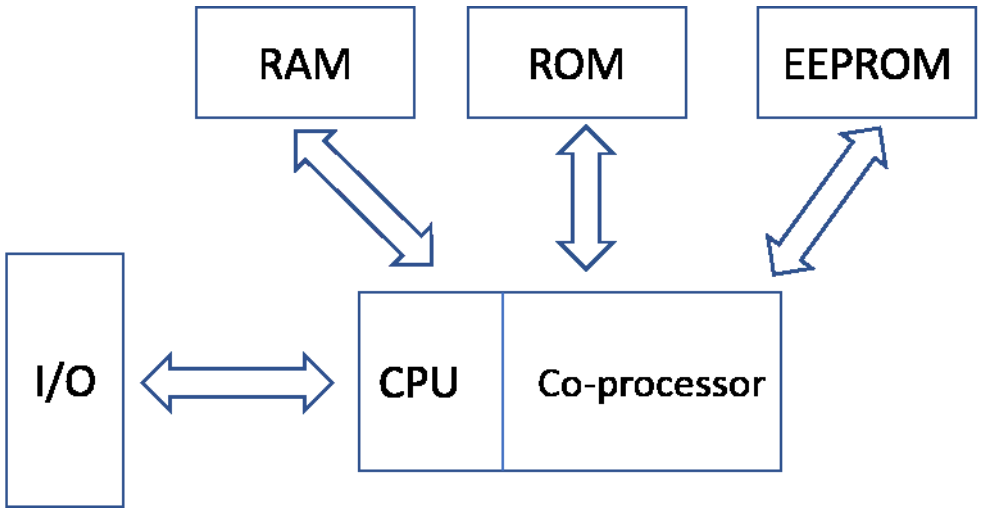

Figure 6: e-ID card embedded chip: components [14]

CPU: The Central Processing Unit in a smartcard functions the same way as in a standard computer, essentially functioning as the brains of the card, controlling and managing functions including memory allocation, file access etc. The CPU also enforces access to the data on the card.

Co-processor: To ensure fast and efficient operation, it is very common for the card to include an on-board PKI co-processor for quick processing of cryptographic functions.

Memory:

RAM: Random Access Memory here works like any system memory and is used as a temporary staging area for running card applications or processes.

EEPROM: The Electronically Erasable Programmable memory as the name implies is used for hosting applications which could be changed at any time, even after the card had been issued to the citizen.

ROM: The Read Only Memory is a non-modifiable memory area used to store the card operating system and other non-changing card applications.

In addition to the components listed above, another important component of the e-ID card is the software platform of the card i.e. Card Operating System (COS). Today, there are two key COS platforms on which the cards run, MULTOS and Java Card. These two card platforms are collectively referred to as a Multi-Application card operating system (MACOS), able to support a variety of applications on a single card, from chip and pin application for payment to on-card biometric matching for secure ID etc. [14].

The MACOS ensures that the card could support multiple applications running on a single embedded chip and from a security perspective, ensure that the applications are clearly segregated. The MACOS also has the advantage of being able to manage the applications on the card even after the cards have been issued [14]. This post-issuance management of card applications is critical to ensure that critical security updates can be made to the cards, in case of any discovered vulnerability long after the cards have been delivered to the citizen i.e. as seen the ROCA vulnerability case affecting Estonia e-ID cards.[14]

3.1.2. Types

Typically, a smartcard provides one of the two communication interfaces: contact and contactless. Most of the systems are based on contact cards but a few recent implementations such as German e-ID card are contactless [4], [14], [44]. Some smart card may provide both the interfaces.

Contact smartcard: Based on the ISO 7816 standard, this type of smart card has electrical contacts which requires that the card's contacts (pins) physically touch (hence their name, contact card) sensors inside a card reader for communication to be possible [14].

Contactless smartcard: Based on the ISO 14443 standard; this type of smartcard does not require any physical contact to communicate with the card reader. Rather, it consists of an antenna with which it could be accessed wirelessly within a short range using electromagnetic induction technologies such as RFID or NFC [4]. Communication within the RF frequency range is at 13.56 MHz and distance (range) is up to 10 cm [14].

Another type is the ***Hybrid card*** which contains two chips, one for contact and another for contactless communication. Another type is a ***Dual interface card*** which utilizes a single chip for providing both functions. Dual interface cards are expected to see more adoption in future e-ID schemes, offering the security of contact as well as the convenience and flexibility of

[14] ROCA: Vulnerable RSA generation (CVE-2017-15361). Retrieved from: https://crocs.fi.muni.cz/public/papers/rsa_ccs17 (Accessed 8/1/2018)

contactless cards (especially as more NFC-compliant smartphones become available which support contactless communication with the card) [14].

3.2. Privacy & security features

The following are some of the many security and privacy preserving features of the e-ID card [29], [30].

Access control mechanisms: The data stored on the cards are often encrypted and a service provider or card reader could access the data only after a successful authentication of the service provider and/or the cardholder (consent). Service providers are sometimes issued authorization certificates which determine the extent to which the service can access the data stored on the e-ID card and what functions can be performed. Citizens also have to give their consent for every access. A successful citizen authentication usually consists of proving knowledge of a PIN or possession of a private key. By correctly entering the PIN, the cardholder authenticates him/herself and gives consent to access data stored on the card.

Secure communication between the card, the middleware and the server: Once the card releases data, it could be vulnerable to eavesdropping while in transit between the card and the middleware interfacing with the card or between the middleware and the destination service. Protocols such as the Extended Access Control (EAC) protocol ensure the mutual authentication of card and reader. Also, a form of end-to-end encryption between card/middleware and the destination service is used to protect the data from snooping while in transit [14], [28], [44], [45].

Privacy-respecting use of unique identifiers (UIDs): To protect end user privacy, it is common for the e-ID cards to use unique identifiers (UIDs) specific to the e-ID system rather than citizen's Social Security Number (e.g. FINUID in Finland rather than SSN [5]) and linkage of the UID to the SSN is done in the issuer's databases.

Pseudonymous authentication: To further strengthen privacy, most e-ID cards support the use of pseudonyms for authentication which, rather than disclose the cardholder's identity to the service provider, discloses only some identifier, uniquely linked to identify the communication section but not the cardholder [29], [30].

Protected memory areas: It is common for the card to have several different memory areas or security zones, depending on security access level required. Examples include a ***Public zone***, for non-privacy critical information such as citizen name, nationality, etc., that is accessible without restrictions, and a ***Private zone***, for more critical data such as citizen biometrics that is accessible only after the user has entered his secret PIN etc. [30].

Selective disclosure: This concept defines that only the minimum data required should be disclosed for a stated purpose. Thus, most e-ID cards only disclose as much information that has been approved for disclosure by the user. For example, if service provider only requires the name of the citizen, the service provider should not be able to read the citizen's Social

Security Number (SSN). In addition, the user may be able to control or limit the amount of information disclosed as seen in the German e-ID card [28].

Verify-only mode: This is a form of selective disclosure, where instead of disclosing actual citizen data, the card responds to a request with a Boolean (True/ False) or Yes/No answer. E.g., if the citizen wants to access an age-restricted service, the card would return a yes or no answer to an age verification request from the service. This way, the service can verify the citizen's age without learning their birth date [28], [30].

3.3. Service description

A typical e-ID service architecture is presented in *Figure 7*. It shows a high-level architecture of the relationship between different stakeholders involved in the e-ID scheme.

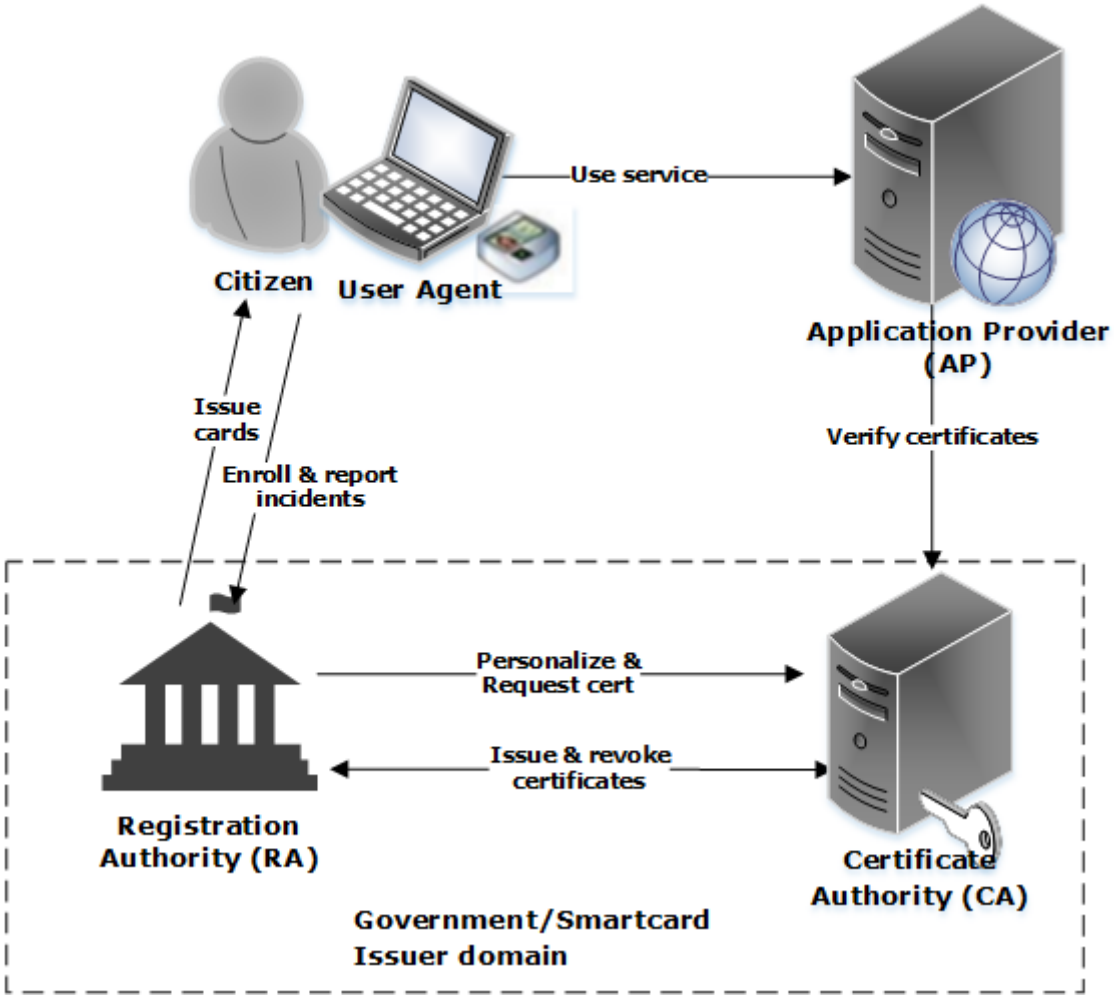

Figure 7: e-ID card Infrastructure: Service architecture

3.3.1. Stakeholders / Roles

End user: The end user is a citizen who acquires and uses the e-ID card. The user applies for the e-ID card in person often by visiting a local registration authority where the user's identity

is verified following the process described in the Certification Practice Statement (CPS) defined by the Certificate Authority.

On receipt of the e-ID card, he/she uses it across different service providers depending on the card use case required.

Application Provider: Also referred to as a Relying entity (RP); an AP is usually a web service provider that uses the e-ID infrastructure for authentication, signing or transaction approval of the user. Application providers include e-government services, e-commerce, online banking platforms etc.

Smartcard issuer (i.e. the government): The government is a common issuer of physical e-ID cards around the world. Typically, a government agency (***otherwise called the smartcard issuer in the e-ID scheme***) is responsible for the e-ID infrastructure. Among its responsibilities are registration, card manufacture & issuance, revocation and overall management of the e-ID infrastructure.

Registration Authority (RA): The RA role is commonly provided by public agencies such as the police or postal service. They provide the registration function for the e-ID infrastructure, verifying and validating the identity of a citizen who wants to acquire the e-ID card. After the citizen's identity has been authenticated, the RA registers the user, personalizes the card and issues the e-ID card to the user.

The RA also provides an incident reporting function, where the citizen could report incidents such as card loss, theft etc. which would trigger the card revocation function. Upon the receipt of such report, the RA requests that the CA revoke the citizen's certificate making the card's e-ID function unusable.

Certificate Authority (CA): The primary responsibility of the CA is to issue (or revoke) certificates for e-ID cardholders. The e-ID scheme Certification Authority infrastructure often comprises multiple CAs, typically arranged carefully in a prescribed order (Root CA, Intermediate CA, and other subordinate CAs in the trust chain). They perform specialized tasks, such as issuing certificates to subordinate CAs or issuing certificates to citizens. The Root CA and intermediary CAs are often owned and maintained by the government for the e-ID scheme, while subordinate CAs could be owned by a private entity.

On the loss or theft of a card, the CA revokes the certificate issued to a citizen and maintains the Certificate Revocation List (CRL) which is a database of revoked certificates. The CA may also issue authorization certificates to e-ID servers communicating with a citizen's e-ID card.

3.3.2. Service flow

A typical application of the e-ID card is described in this section. An example application is an authentication process for granting access to a web service using an e-ID card. The process steps taken includes:

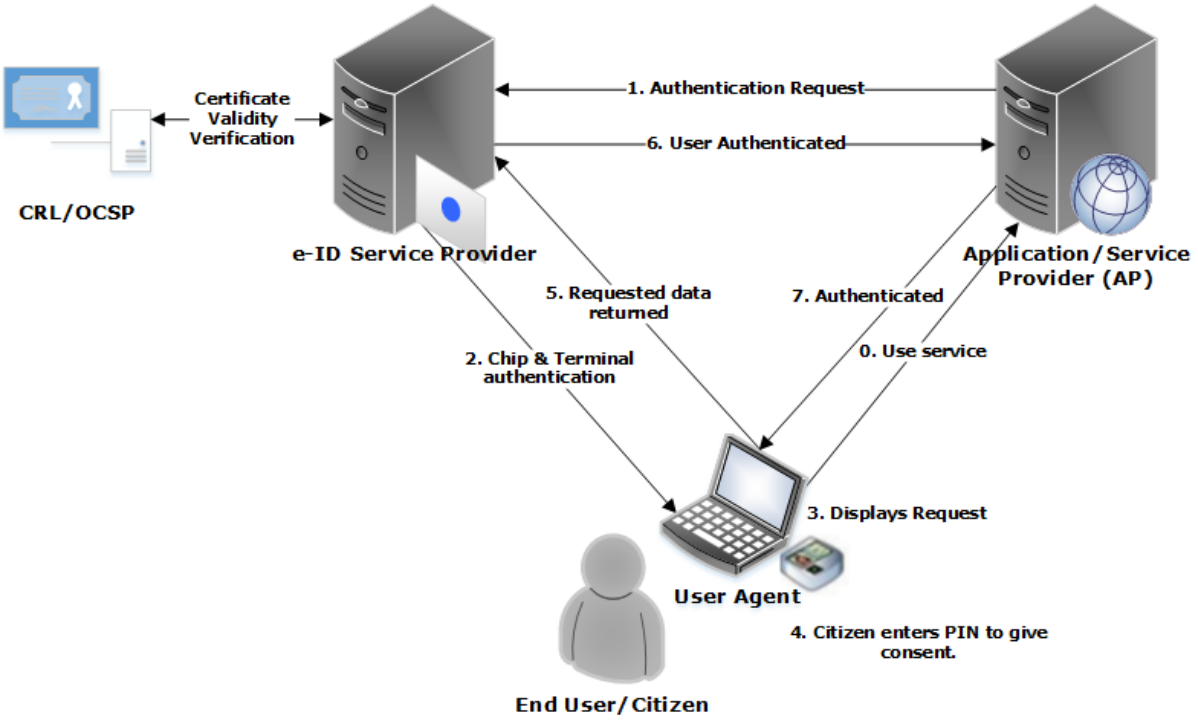

Figure 8: e-ID Service (Authentication) flow [22]

0. A user accesses an online service that requires authentication and selects the e-ID Card as the method of authentication.

1. In the backend, the web service sends an Authentication request to an associated e-ID infrastructure (e.g. provided by an e-ID service provider) or the client-side e-ID card reader software.

2. Mutual Authentication: The client-side software mediates a mutual authentication between the e-ID infrastructure (or web service) and the ID card to establish a trusted communication channel.

3. Display of Service Info & Request: The client-side e-ID software receives and displays information about the service and request. The user is advised to enter the e-ID Card in the card reader if not already inserted. Security warnings and other information could also be displayed if needed.

4. Consent: The user is then prompted by the client-side software to enter the PIN for the certificate to complete the service request. Depending on the type of service, the PIN choice could be different (e.g. PIN1 for the authentication or PIN2 signature certificate). After reviewing the displayed service information, the user enters the corresponding e-ID PIN to give consent.

5. In case the PIN is correct, the e-ID server (or web service) reads the authorized subset of data from the e-ID card. The certificate validity is also verified in the backend using a Certificate Revocation List (CRL) or through an OCSP query service provided by the CA.

6. If the validity verification is successful, and the user's certificate is valid, the authentication data along with the requested identity attributes are returned to the web service. Information returned to the web service may also be displayed to the user.

7. After the authentication process is completed, the web service resumes control and uses the authentication results for its purposes i.e. the user is signed in to use the service.

3.4. Example implementations

Today, physical e-ID cards are the most popular and deployed strong e-ID solution in the world.[15] Countries to have introduced physical e-ID cards include Finland, Germany, Belgium, Bulgaria, Chile, Guatemala, Israel, Italy, Luxembourg, the Netherlands, Nigeria, Mexico, Morocco, Pakistan, Portugal, Romania, Estonia, Latvia, Lithuania, Spain, Slovakia, Malta, Mauritius to mention a few [4].

In the subsequent sections, the e-ID card schemes from Finland (using contact cards) and Germany (using contactless cards) are briefly surveyed.

3.4.1. FINeID

As stated in the opening part of this chapter, the FINeID is the first smartcard based national e-ID card implementation in the world. The goal of FINeID is to provide a means of electronic identification to all citizens and permanent residents in the country. It was launched to the public in 1999 as a non-mandatory electronic identity card with the Finnish Population Register Centre (PRC, Väestörekisterikeskus in Finnish) serving as the card and certificate issuer [5].

Figure 9: Example FINeID card

FINeID is an acronym for FINnish electronic IDentity.[16] The FINeID card is an ISO 7816 standard based contact e-ID card. The card front contains user identity data such as full name, photograph, date of birth and social security number (SSN), gender, nationality, if Finnish and null (XXX) if citizen of foreign country, user signature, card number and card validity period. In addition to these, the card also contains a machine-readable zone (readable by an optical

[15] *Electronic identification.* Wikipedia.
[16] VRK "*FINeID.*" Retrieved from: http://vrk.fi/en/certificates-fineid (Accessed 10/02/2018)

character recognition (OCR)), as well as an optional QR code for the Finnish Social Insurance service on the back of the card.

The Finnish Population Register Centre is responsible for the e-ID card manufacturing, card personalization and creation of PKI keys, issuing and storage of certificates. In cooperation with the Finnish police, application and registration for the card, card distribution, card and certificate revocation, maintenance of certificate revocation lists etc. belong to their responsibility [43]. The FINeID Card is valid for 5 years from the date of issuance and could be renewed on/before/after expiry upon application by the cardholder.

The FINeID card establishes an electronic identity (e-ID) based on the information contained in the Population Information System (Väestötietojärjestelmä), where a key set of authentic identity attributes for all Finnish citizens and permanent residents in Finland is maintained. All the electronic attributes stored on the e-ID card are obtained directly from the Population Information System [5], [43]. Stored attributes include:

- Name comprising of the last name and given name(s) of the cardholder.
- Citizenship - Abbreviation for cardholder's country of origin.
- Unique identifier of subject in Finland (FINUID/SATU): The Population Register Centre (PRC) issues a Personal Electronic Identifier (SATU in Finnish) to Finnish citizens and permanent residents upon the creation of a social security number (HETU in Finnish) [55]. The privacy sensitive social security number (HETU) is not stored as one of the attributes on the e-ID card. In place of the HETU, a privacy respecting unique identifier (SATU) is stored electronically. SATU is mapped to the corresponding HETU (retrieved from the Population Information System) to establish user identity. The user is required to give their consent (by entering the PIN) before this mapping can be done.
- Optionally, the cardholder could also choose to store an email address on the card. The e-ID does not contain any biometric information.

According to the FINeID specifications[17], there are two PKI key pairs on the FINeID card for a user. The two X.509 user certificates are for authentication and non-repudiation. The authentication certificate is used for authentication and encryption (using the private *'auth. and encipherment'* key). The 'auth. and encipherment' key length is RSA 2048 bits and is protected by a 4-digit PIN 1. The non-repudiation certificate is used for signing (via the *'signature'* key). The 'signing' key length is RSA 2048 bits and is protected by a 6-digit PIN 2. A Personal Unblocking Key (PUK) is provided for Unblocking both PIN 1 and PIN 2. The Signature/non-repudiation certificate is a qualified certificate. The PRC is currently the only CA who issues qualified certificates in Finland [55].

[17] VRK "*FINEID-specifications*." Retrieved from: https://eevertti.vrk.fi/en/fineid-specifications (Accessed 10/02/2018)

In addition to the two user certificates, the FINeID card contain two X.509 CA certificates. (1) For the Root CA (named, VRK Gov. Root CA), and (2) an intermediate CA certificate (VRK Gov. CA for Citizen Qualified Certificates) signed by the Root CA. The Root CA certificate key length is RSA with 2048 bits and the intermediate CA certificate key length is RSA 4096 bits.

The Citizen certificates meet the requirements for qualified certificates defined in the EU eIDAS Regulation.[18]

Penetration

Although there have been no recent penetration figures on the FINeID card published by the Finnish Population Register Centre, compared with the Estonia e-ID card, the FINeID card project has not been quite as successful as expected. Today, penetration rate is estimated at only around 10% of the over 5.5million population of Finland,[19] compared with up to 98% of Estonians holding the Estonian e-ID card.[20]

Among the factors cited for the low popularity of the FINeID card are, availability of cheaper, more convenient options such as TUPAS and Mobiilivarmenne, lack of card readers, cost of the card and difficulty of use (poor card reader software), among others. Another limitation mentioned was the refusal of banks to allow the use of the FINeID card for authentication on their platforms. All of these factors mean that the FINeID card finds more use in physical world identification than on the Internet.

3.4.2. German e-ID

The German e-ID is the national e-ID card issued by the German government, with issuance starting in 2010. It is a card issued to all German citizens, with a similar e-ID feature also available on German resident permit cards. The e-ID card is a contactless chip card based on the ISO/IEC 14443 and ISO/IEC 7816 standards [44], [45]. The technology of the German e-ID is based on the EU eIDAS token specification, defined in several guidelines listed in [45].

The card front is like in the FINeID and contains user identity data such as full name, photograph, date of birth, gender, nationality, user signature, cardholder's address etc., card number and card validity data. In addition to these, there exists a machine-readable zone (readable by an OCR) on the back of the card.

---

[18] VRK. "*Information about certificates."* Retrieved from: https://eevertti.vrk.fi/en/about-certificates (Accessed 10/02/2018)

[19] Wikipedia. "*Finnish identity card."* Retrieved from: https://en.wikipedia.org/wiki/Finnish_identity_card (Accessed 10/02/2018)

[20] e-estonia. "*id card."* Retrieved from: https://e-estonia.com/solutions/e-identity/id-card/ (Accessed 20/04/2018)

Figure 10: German e-ID card [45]

The German e-ID card is designed to meet the requirements for a qualified electronic signature creation device as defined in the EU eIDAS regulation. The chip of the German e-ID card stores the personal data of the holder and serves as tamper-resistant device protecting the stored data from unauthorized access. The German e-ID card provides the following functions [28]:

ePass: The ePass function in the German e-ID card works like an ePassport; It contains cardholder's biometric information which is accessible only by public authorities for identity check e.g. police, border control etc. but not including e-gov., services. Attributes stored in the ePass include:

- A digital photograph
- Serial number and
- Fingerprints (optional)

The second function provided by the German e-ID card is an **e-ID function**, available to anyone over the age of 16**.** It is an Attributes-based credential used for online identification and authentication of a natural person. The card is accompanied by a six-digit PIN which the user must enter to give their consent before a service provider is allowed access to the data stored on the card. The user could also restrict the amount of data a service provider can read before granting read consent [28], [44].

The e-ID functionality enables the secure electronic identification of the cardholder based on a two-factor authentication, i.e. Possession (e-ID card) and knowledge (PIN). Stored attributes in the chip of the card for the *e-ID function* include [28]:

- Name comprising of the family name and given names,
- Date of birth and place of birth,
- Card holder's address and postal code,
- Type of document,
- Card validity (Expiry date),
- Service and card specific identifier (for pseudonymous authentication),

- Indication of card holder's age (for verify-only requests),
- Indication of place of residence matches a particular address, and
- Optionally, the cardholder could choose to include the following, including Name at birth, doctoral degree and religious name / stage or pen name.

Digital (Qualified) Signature: The German e-ID card includes an opt-in qualified signature function where the citizen could purchase a signature certificate from qualified trust service providers authorized by the Federal Office for Information Security (or Bundesamt für Sicherheit in der Informationstechnik, in German, abbreviated as BSI) to issue such certificates. This function after activation could be used to sign documents electronically such that the signed document has the same legal backing as a handwritten signature [44].

Cryptographic protocols secure the channels between the card and the reader and between the card and the e-ID server. Between the card and the reader, the Password Authenticated Connection Establishment (PACE) protocol is used to verify the cardholder's PIN and to establish a secure channel of communication between the e-ID card and the card reader. Mutual authentication between the card and e-ID server is achieved through the Extended Access Control (EAC) protocol [45]. According to [28], the Cryptographic algorithms used in the German e-ID card include the following:

- AES-128 CBC (cipher block chaining) and CMAC (cipher-based message-authentication code) for messaging security;
- SHA-256 for hashing;
- elliptic-curve Diffie-Hellman for key establishment in PACE, chip authentication, and restricted identification; and
- Elliptic Curve Cryptography with 256-bit curve (e.g. Brainpool). ECDSA (Elliptic Curve Digital Signature Algorithm) for authorization certificates and signatures.

Penetration

Possession of the German e-ID is mandatory for all adults in Germany. Thus, as expected, the German e-ID card has a good penetration figure among the German population. According to Gemalto, who is a major supplier for the German e-ID cards, more than 51 million cards have been distributed as of June 2017.[21] The e-ID function on the card is usable with all municipal and national government services. However, it was also reported that only around 30 - 35% of the distributed e-ID cards has activated the e-ID function.[22] [23]

It is expected that as more government services become available online, more people will activate their cards for use at these services.

---

[21] Gemalto. "*Overview of the German identity card project and lessons learned (2017 update).*" Retrieved from: https://www.gemalto.com/govt/inspired/eid-in-germany (Accessed 20/04/2018)

[22] *Ibid.*

[23] Eike Kühl. "Das tote Pferd soll auferstehen (in German)." Retrieved from: https://www.zeit.de/digital/datenschutz/2017-04/elektronischer-personalausweis-eid-gesetz-biometrie-datenbank (Accessed 25/07/2018)

3.5. Use cases

The e-ID card acts as an identifying device enabling access to various online services. The main driver for a national e-ID scheme was built on an interest by governments to deploy e-government services. Depending on the level of security assurance required, the e-ID card offers access to different types of services. Among some of the applications of the e-ID card are:

Identification & Authentication – This uses the attributes stored on the e-ID card to deduce who the cardholder is. The stored attributes are then used to corroborate the claimed identity by the person looking to perform the operation (is the person same as the cardholder?). The person must know the authentication PIN of the e-ID card to enable access to the stored attributes. Examples of applications include the following, among others:

1. Enabler of e-government and proving a citizen's identity for an e-government application including eTaxation, eVoting, eHealth, electronic social services etc.
2. Opening a bank account. To meet KYC requirements, thereby enabling online banking.
3. Registering & signing in to an eCommerce site.
4. Anonymous & pseudonymous authentication for social media.
5. Strong & multi-factor authentication for online banking and e-government services.

Non-Repudiation – This uses the digital certificates on the e-ID card to express the will of the cardholder to perform a particular operation. The produced digital signature enables the service provider to establish the authenticity of data and cardholder's identity such that a verifiable proof of transaction could be produced. Examples of applications include:

1. Electronic Signature, such as signing a document e.g. a tax form.
2. Transaction Approval e.g. making a payment, etc.

3.6. Limitations

Cost: Compared with competing solution such as Bank credentials (BankID), the e-ID card is expensive to the end user. Firstly, users have to pay to acquire the e-ID card (e.g. 55€ for the FINeID card and between 22 and 100€ for the German e-ID card). In addition to the cost of the cards, users also have to invest in card readers to be able to use their e-ID cards. Compared with the BankID, which is often available free of charge from the user's bank, it does not make economic sense for the user to acquire the e-ID card while the BankID is available.

Convenience: One major limitation of the e-ID card is the convenience of use on the part of the end user, thereby when compared with other solutions available (e.g. BankID or Mobile PKI); e-ID cards offer worse user experience. The e-ID card constitutes an extra device that the user has to have on them, while the card reader constitutes another. The unavailability of one of these devices means that the user is unable to complete the needed transaction. This severely affects the application of the e-ID card for on the go use.

The main motivation for the national e-ID card is application for e-government services, especially when there are no alternative solutions available. When there are competing, simpler and more convenient solutions available, the e-ID cards are mostly not attractive to the consumers as seen in the case of FINeID card [5].

Another challenge facing the adoption of e-ID cards is the little or no awareness to the end user of the clear benefits in using digital signatures. Thus, end users are happy to use less secure solution such as bank credentials for authentication for all their online applications.

Chapter 4

Mobile PKI

The most important requirements for online services when it comes to the electronic identification solution include [58]:

- Easy to set-up,
- Cost-efficient,
- Legally acceptable,
- Open and interoperable,
- Mobile and ubiquitous, and
- Global in scope (could reasonably reach different countries/languages, devices etc.)

A review of competing solutions shows that a lot of them come short in meeting these requirements. An e-ID solution based on mobile phones promises an easy solution to meet these requirements.

Mobile phones, today, are not just for making phone calls anymore. The use of mobile phones has spread to other areas such as email, gaming, banking, video streaming, and most importantly social media. In fact, mobile phones and technologies have become a huge disruptor in the world today. For example, the social media world that we live in today is driven in large part by the pervasion of mobile devices with huge processing power, commonly referred to as smartphones. They are unarguably the main driver for the adoption of e-services today; thus, the current explosion of demand for strong authentication on the Internet is in part driven by smartphones.

At the end of 2017, the number of unique mobile subscribers was estimated to be over 5 billion, almost 70% of the world's population. This figure is expected to have risen to 6.1 billion by 2023 according to Ericsson Mobility Report released in June 2018 [48]. Mobile phone devices are now the most deployed end user device type in the world, able to reach even the most remote and under developed locations on earth.

What we have with this penetration figure is that through the mobile phone, a highly secure tamper-resistant device, the SIM/USIM card is readily available to more than 5 billion of the world's population. The high penetration rate means that the usage of the mobile device can evolve to include even more applications - one of which is strong electronic identification.

An e-ID solution based on mobile devices is attractive due to the following features:

- Almost everyone in the world today, already has a phone, therefore, there is no need for additional devices like PKI tokens, OTP tokens, smart cards etc.
- According to ETSI [49], the worldwide penetration of the mobile phone makes it the cheapest and most convenient choice for delivering a socially inclusive and truly mass-market e-ID solution.
- The mobile phone has become a complete part of people's lives, a device that is always with them. This means that an e-ID solution available through the mobile phone could be readily available for use on the go and at all time.
- A mobile phone provides the important functions required for its usage as a device for strong electronic identification including the tamper-resistant smartcard that could be used for PKI operations and certificate storage and the card reader able to access the data stored on the smartcard.
- Roaming and interoperability is built into mobile network technology meaning that such e-ID solution could also be used when a subscriber is roaming in a network other than their home network.
- The mobile network has built-in security mechanisms in which it allows only authenticated devices to connect to the network.

The discussions to define an e-ID solution based on mobile phones began in the late 1990s to the early 2000s. The European Technology Standards Institute (ETSI), signaled the maturity of the discussions in 2003, when it defined a solution based on Mobile devices, called Mobile Signature Service (MSS, also referred to as Mobile PKI or Mobile ID). ETSI defined a Mobile Signature as "A universal method for using a mobile device to confirm the intention of a citizen to proceed with a transaction".

ETSI defined MSS through the following Technical Reports (TR) and Technical Specifications (TS):

- ETSI TR 102 203 [49]: "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements." This TR presents a non-technical introduction to mobile signature services, as well as business and functional requirements for the solution. It also describes a large number of application scenarios and contains a justification of the design criteria and a possible way to assign the various roles.
- ETSI TS 102 204 [50]: "Mobile Signature Service; Web Service Interface." This TS describes the communication interface as well as the syntax of the messages exchanged between the MSSP (MSS server) and relying Application Providers (APs).
- ETSI TR 102 206 [51]: "Mobile Signature Service; Security Framework." This TR defines the security requirements for an MSS solution.
- ETSI TS 102 207 [52]: "Mobile Signature Service; Specifications for Roaming in Mobile Signature Services." This TS defines the ETSI standards for MSS roaming, allowing MSS service requests to roam between a number of MSSP servers.

The TRs and TSs together define the requirements for the design and implementation of MSS or Mobile PKI solutions.

As defined by the ETSI standards, Mobile PKI uses mobile phones to implement a strong electronic identification solution, leveraging the tamper-resistant secure element in the phones. It works on the same principles as in physical smartcard-based solutions such as the government issued e-ID cards surveyed in Chapter 3. However, the solution does not require an extra smartcard device or card reader. Rather, the solution utilizes SIM/UICC cards inside mobile phones and the mobile phone itself functions as the card reader [49], [53].

The SIM card based mobile PKI solution offers a strong electronic identification for end users as required by application providers. The combination of two-factor authentication (What the user has; "their phone" and what the user knows; "their unique PIN"), with messages exchanged over two separate communication channels (IP for application provider access and SMS for signature operations) makes tampering or corrupting the transaction inherently a lot more difficult than in most other solutions [61].

4.1. Technical & security features

Mobile PKI involves the utilization of PKI on mobile devices. In a Mobile PKI implementation, the client-side mobile device has a secure element (e.g. SIM card) that holds the private key. The public key is stored in a certificate on the server-side MSSP during registration [58].

The Mobile PKI infrastructure is divided into two parts/sides as shown in the Figure 11 below:

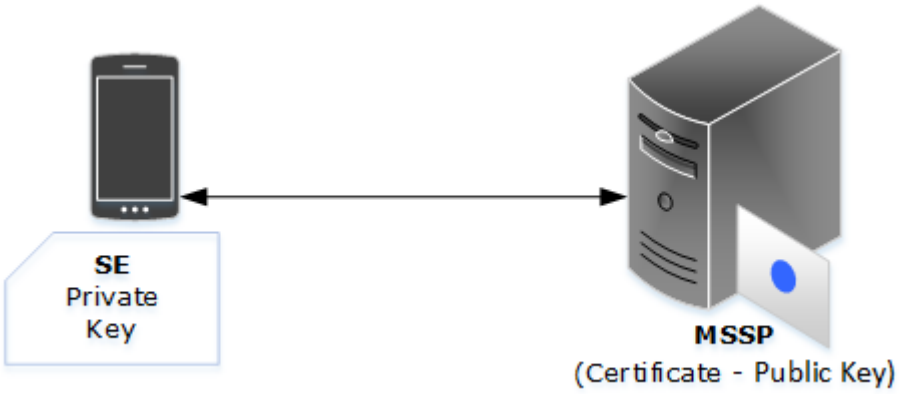

Figure 11: Mobile PKI system [58]

- Client-side tamper-resistant Smartcard (SIM/USIM) and
- Server-Side Mobile Signature Service Provider (MSSP).

4.1.1. Client-side SIM / UICC card

The client side is composed of the Signature Creation Device (SCD). This includes the tamper-resistant smartcard and the wireless PKI application that perform all functions related to signature creation and signature services.

The Subscriber Identity Module (SIM, used in GSM network) or Universal Integrated Circuit Card (UICC in UMTS networks) forms the client side for MSS solutions. The SIM card[24] is an integrated circuit chip embedded in a physical card intended to securely store data about mobile subscribers, including the international mobile subscriber identity (IMSI) number, network authorization data, personal security keys, contact lists and stored text messages etc. [57].

The SIM card is well established as a tamper-resistant security device in mobile telecommunication networks. Its primary purpose is to identify and authenticate a mobile subscriber in a mobile network in a secure and consistent way. It offers security, privacy, and trust functionality for mobile services with applications far beyond the primary voice traffic [57].

The SIM card has come a long way since the introduction of the GSM in the early 1990s and has evolved in size and capabilities along with the mobile network technology itself. Based on the ISO/IEC 7816 standard defining the physical characteristics of Identification cards. Figure 12[25] below highlights the SIM card size shrinkage over the years to the most common distribution size today, the Nano SIM based on ETSI TS 102 221 V11.0.0 standard.

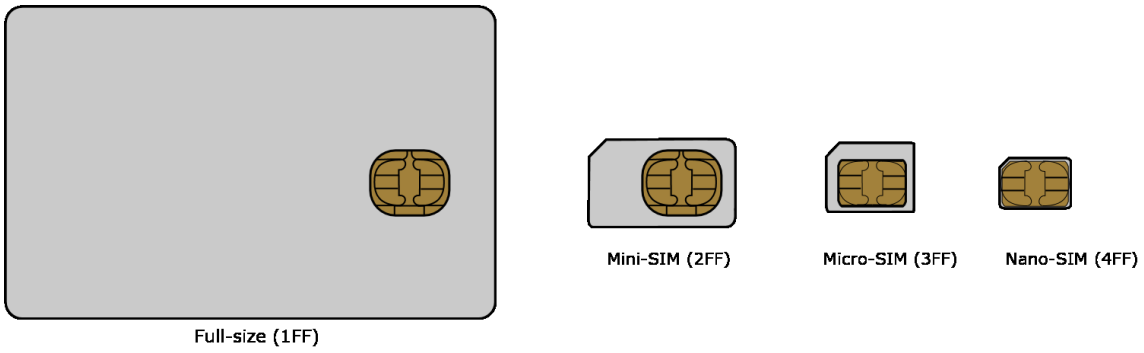

Figure 12: SIM card evolution

Today, the SIM card is a miniaturized tamper-resistant smartcard that fits conveniently inside a mobile phone. Over the next couple of years, it is expected that the physical SIM card will disappear completely to give way for an embedded chip (eUICC/eSIM) inside the mobile device.

Mobile PKI requires a suitable SIM card. Specifically, a SIM card with a dedicated hardware processor optimized for cryptographic operations and key generation (i.e. cryptographic processor), sufficient memory, and with a Wireless Public Key Infrastructure (WPKI) SIM Toolkit (STK) application installed. The cryptographic processor on the PKI SIM card allows the card to perform complex cryptographic operations including key generation on board the card, storage of keys and other processing operations required in the mobile signature service [53], [54], [58], [62].

---

[24] Wikipedia. "*Subscriber identity module.*" Retrieved from: https://en.wikipedia.org/wiki/Subscriber_identity_module (Accessed 2/1/2018).
[25] Ibid.

The PKI SIM by design meets the requirements for a qualified electronic signature creation device, as defined in in Annex II of the EU eIDAS regulation. It provides a tamper-resistant environment for storing end user's cryptographic credentials.

The SIM card like any smartcard includes a number of internal components as shown in the Figure 13 below, with only components relevant to Mobile PKI highlighted.

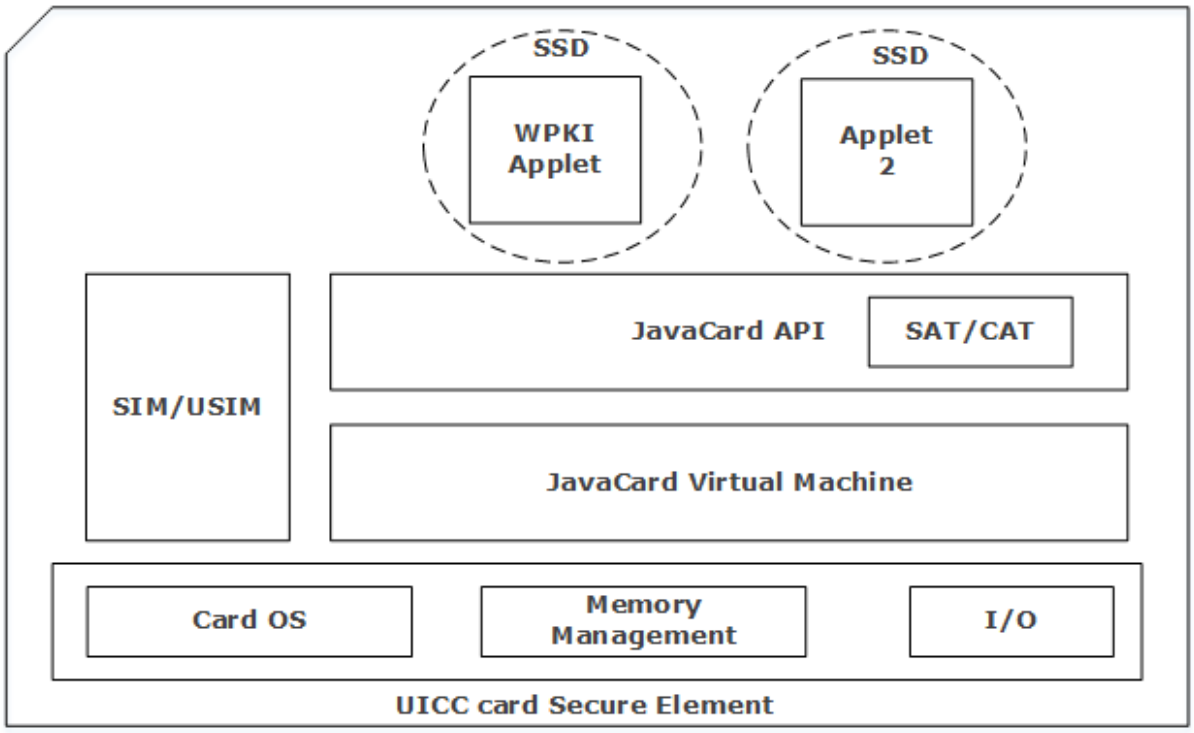

Figure 13: SIM card internals

Card OS: The most commonly deployed SIM card OS today is JavaCard. JavaCard is a multi-application card operating system that allows the deployment of various applications (referred to as applets) atop the SIM card. It also provides a secure execution environment for the applets deployed on the SIM card and includes two specific APIs, JavaCard API and SIM Toolkit API [53].

The ***JavaCard API*** includes a set of classes and methods that enable and perform both the key generation and signature processes, based on the cryptographic capabilities of the SIM card. It provides a platform upon which the JavaCard applet for Mobile PKI is deployed.

The WPKI applet communicates with the mobile phone using – ***SIM Application Toolkit*** (SAT or CAT in UICC cards). The SIM/Card Application Toolkit (SAT/CAT) defines a complete set of commands and events between a mobile phone and the SIM card, independent of mobile devices or card manufacturers. These allow the applications on the SIM card to communicate and display different dialogs and menus on the screen of the device to the end user [53].

WPKI Applet: - This is a JavaCard signing (PKI) application (referred to as an Applet), deployed in the SIM card. The WPKI applet enables electronic signature creation on the SIM card. The WPKI applet is deployed into a separate security enclosure, referred to as a Supplementary Security Domain (SSD) with its own cryptographic keys that allows only authorized entities to communicate with the applet [58], [62]. The Mobile PKI menu generated

by the WPKI applet is located in the “Extra”, “Tools” or “SIM Toolkit” menu on the mobile phone.

The WPKI applet enables the mobile phone user to receive signature requests and by entering the correct PIN for the private keys stored on the SIM card, produces a valid signature response [58], [62]. Today, the most common signature algorithms used in Mobile PKI are the RSA algorithm with either 1024bit or 2048-bit key length or ECC with a 256-bit curve. Examples of WPKI applet for Mobile PKI include Alauda WPKI applet by Methics Oy, VMAC applet by Gemalto (previously Valimo) and WIB by G&D.

4.1.2. Server-side Mobile Signature Service Provider (MSSP)

The Mobile Signature Service Provider (MSSP) platform forms the server-side implementation of the Mobile PKI system. It is an intermediary between users and Application Providers (APs), facilitating communication between the AP and the WPKI applet on user’s SIM card. It enables mobile signature services for APs and end-users. The MSSP platform handles the signature request and response process, communication with the WPKI applet in the mobile phone, signature validation and transaction management covering the whole signature transaction lifecycle [58], [62].

The MSSP platform according to the ETSI specification typically consists of a Home MSSP, AE (acquiring entity) MSSP, ME (Management entity) MSSP and possibly an RE (routing entity) MSSP [49], [58].

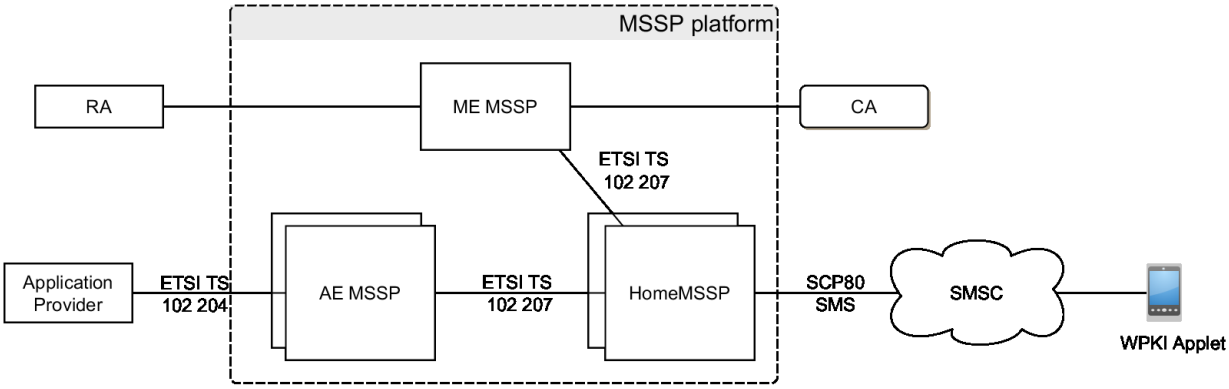

Figure 14: MSSP platform [58]

Application Providers seeking to utilize Mobile PKI for strong electronic identification and authentication connects to the Mobile PKI system through the ***AE MSSP*** over the ETSI MSS SOAP protocol (ETSI TS 102 204). The AE MSSP retrieves a request from the authorized AP, determines the destination Home MSSP from the user’s MSISDN included in the request and sends the request message forward to the Home MSSP.

The ***Home MSSP*** handles the communication between the WPKI applet on the user’s SIM card and the AE MSSP. It connects to the AE MSSP over the ETSI MSS roaming protocol (ETSI TS 102 207). It connects to the operator’s wireless network and communicates with the WPKI applet over bearer channels such as SMS (Short Message Service) (most popular), USSD (Unstructured Supplementary Service Data), BIP (Bearer Independent Protocol),

CAT_TP (Card Application Toolkit Transport Protocol) etc. It ensures the security and privacy of messages to and from the SIM card by using encryption keys to protect the messages.

The ***ME MSSP*** provides a secure registration and management solution for both APs and Mobile PKI users. It provides interfacing tools for integrating the RA and CA systems in the Mobile PKI infrastructure.

The ***RE MSSP*** provides connection to other MSSPs in a mesh Mobile PKI system.

Together, the AE, ME and Home MSSP provide the server-side infrastructure required in the Mobile PKI system.

4.2. Security & privacy features

Like the e-ID card, the Mobile PKI infrastructure, implements security and privacy preserving features including, Pseudonymous authentication, Selective Disclosure, Verify-only mode etc. Other particular security and privacy features of Mobile PKI include the following [53], [54], [57], [58]:

Isolation: The WPKI applet is deployed in a separate security zone (SSD) on the SIM card with its own protected memory area. Using SSD for the WPKI, with separate cryptographic keys ensures that no application on the SIM card or unauthorized entity can access the applets memory area or data.

Onboard Key generation: The combination of the signature creation device (SIM card) and the WPKI applet allows the PKI key pairs to be generated inside the card, and the private keys on the cards never leave the card. This helps to prevent the possible security vulnerability caused due to card / Key / PIN logistics required for example in the case of the e-ID card.

Private Key protection: The Mobile PKI private keys are protected with a PIN which is defined by the user when the PKI keys are generated. The user expresses consent for each transaction by entering the PIN protecting the private key used for the requested transaction.

Secure communication: Mobile PKI employs encrypted SMS text messages to communicate between the MSSP and SIM card (WPKI Applet). This includes using Over the Air (OTA) transport keys (GSM 03.48) and other proprietary transport encryption mechanisms to ensure end-to-end message integrity [51], [58].

Mutual authentication: According to the ETSI MSS specifications, all connections must use mutual TLS authentication. The security of communication between the application provider and the MSSP is thus, ensured through shared communication addresses, mutual TLS authentication of the entities and message integrity based on XML signatures. This trust model is based on SSL/TLS X.509 certificates securely shared between system entities. This also ensures that only authorized and mutually authenticated APs could request for a mobile signature using the Mobile PKI system [51].

On device security: The security of the user interface for user interaction is ensured under GSM and SAT standards. Before a request is displayed to the user via a prompt, a trusted path is established between the SIM card / WPKI applet and the host mobile phone. This ensures that untrusted applications cannot intercept or modify the user's input [51].

Transaction security: The Mobile PKI also implements additional security features to ensure that what the user signs is the same data they intended to. The Application provider is required to display an event ID (on its web interface) and include the same event ID in the request (DTBD). Through the event ID, the user is able to know when accepting a signature request exactly which event the signature request is related to [51].

The ETSI specifications also guarantee that what the user signs (Data to be Signed – DTBS) is the same as the Data shown to the user (i.e. Data-to-be-displayed – DTBD); otherwise referred to as *"What-you-see-is-what-you-sign"*. This ensures that the user can be relatively sure that what they signed is exactly what they intended, and it could not be modified thereafter.

4.3. Service description

A typical Mobile PKI service architecture is presented in Figure 15 below. It shows a high-level architecture of the relationship between different stakeholders involved in the WPKI.

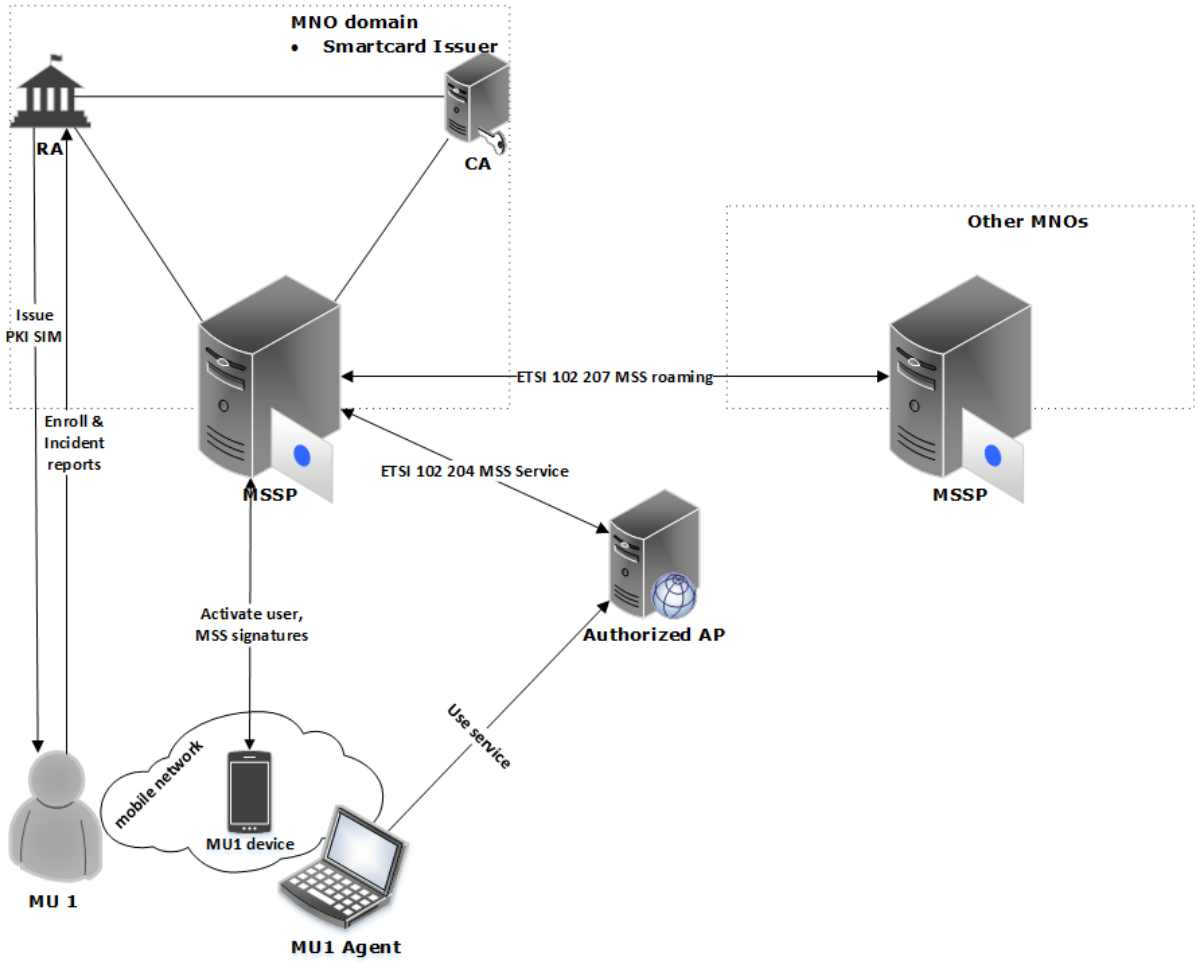

Figure 15: Mobile PKI Service architecture

4.3.1. Stakeholders / Roles

End user*:* Referred to as the Mobile User (MU in Figure 15 above) in MSS terminology. The end user is a subscriber of Mobile PKI who upon registration acquires a Mobile certificate that could be used for the strong identification/authentication of the user with different service providers accepting Mobile signatures.

Authorized AP: Also referred to as a Relying entity (RP); an AP is usually a web service provider that has been authorized by the MSSP and could use the Mobile PKI infrastructure to strongly authenticate or identify the user. Application providers include any e-service providers such as e-government services, e-commerce platforms, banking institutions, educational institutions etc.

Smartcard issuer: The smartcard issuer in the Mobile PKI infrastructure is the Mobile Network Operator. The secure element in Mobile PKI (i.e. SIM card) is the property of the mobile network operator who controls access to the card. The MNO is responsible for the issuance and lifecycle management of the card. In practice, the MNO is mostly also responsible for the corresponding Mobile PKI infrastructure, which includes both the server-side and client-side implementations described above. In addition to the SIM card and MSSP, the MNO also provide the RA and CA functions.

Registration Authority (RA): The responsibility of the RA in Mobile PKI is the same as found in physical e-ID card implementations. It involves the authentication and verification of the intending Mobile PKI subscriber's identity and thereafter registration to the Mobile PKI system. This role is often located in the MNO's CRM (Customer Relationship Management) function and includes the issuance of a suitable PKI SIM card to the user.

The RA also provides an incident reporting function, where the user could report incidents such as SIM loss, theft etc. which would trigger the Mobile PKI account deactivation and certificate revocation.

Certificate Authority (CA): The certificate authority's (CA) function in Mobile PKI includes certificate issuance and revocation for a registered end user. It also maintains a Certificate Revocation List (CRL) or OCSP query service, through which the validity of certificates could be verified.

4.3.2. Service flow

A typical Mobile PKI service flow is as shown in Figure 16. The use case could be a simple authentication to an online service provider, bank transaction approval or an electronic document signing application.

Before an application provider could use the Mobile PKI service, it is required to first acquire a service agreement with the MSSP platform provider (e.g. MNO), acquire authorization and SSL certificates for mutual authentication with the MSSP. Thereafter, the AP could begin to request signature services from the MSSP for user consent to complete a transaction. The following flow and process steps below describe a typical Mobile PKI authentication service [49], [56], [59].

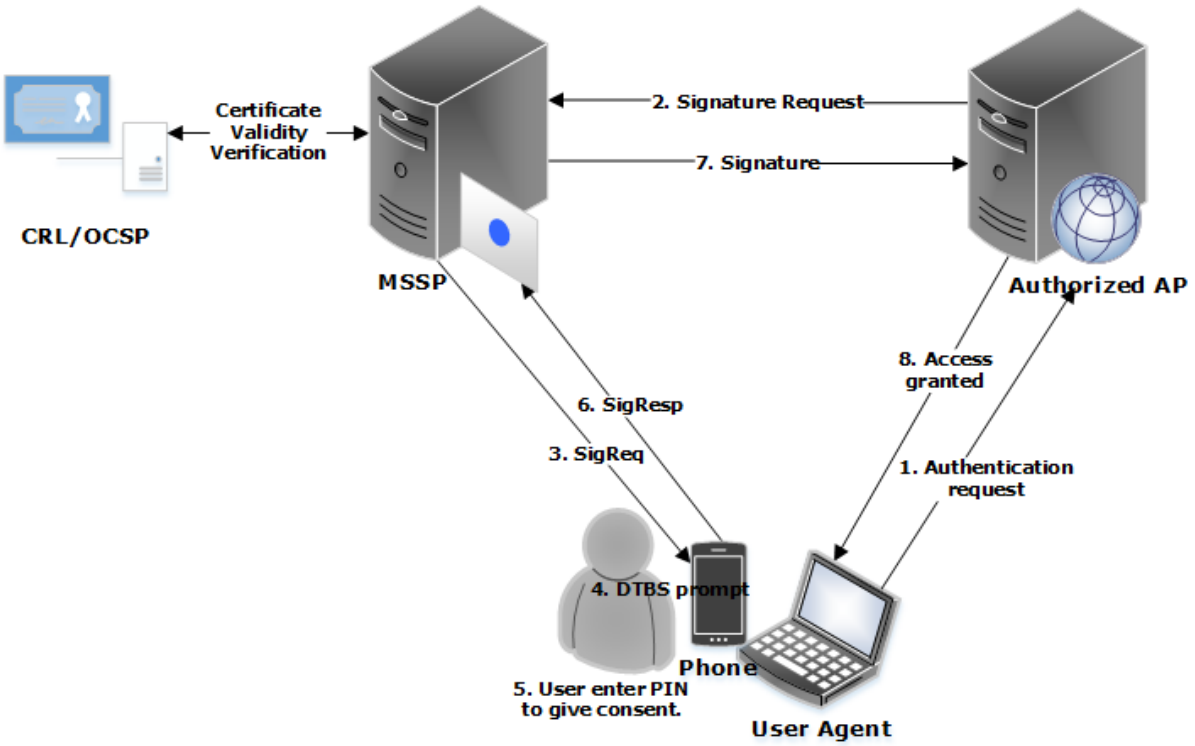

Figure 16: Mobile PKI Service usage flow

1. A user accesses an online service provider application that requires authentication and selects Mobile PKI as the preferred method of authentication. The user enters the mobile telephone number (MSISDN) of his/her phone to receive the signature request.
2. The Application provider sends a Signature Request (SigReq) with the destination MSISDN to the Internet/AP facing AE (Acquiring Entity) MSSP. The AE MSSP checks the SigReq ensuring it is in the correct format and determines the Home MSSP of the subscriber. The AE thereafter forwards the request to the correct Home MSSP.
3. The Home MSSP receives the request from the AE and forwards the request to the end user's phone using an encrypted SMS message.
4. The SIM card receives the request and the user is prompted to enter his/her Mobile PKI PIN to give consent to complete the transaction. The prompt could also include an Event ID matching the one displayed on the application provider's webpage.
5. The user reads the request text displayed, accepts the request by pressing OK and enter the corresponding PIN for his/her authentication key.
6. A signature response (SigResp) is sent to the MSSP, who verifies the validity of the signature by querying the CA (using CRL/OCSP) for the validity of the user's certificate.
7. If valid, the MSSP returns the signature response containing the user identity and other possible attributes to the Application provider. The Signature Response contains the public end-user certificate that corresponds to the private key in the SIM card. The AP is also able to verify that what was signed was the original challenge it sent to the MSSP.
8. Finally, the user is granted access to the application.

The flow for signing or transaction approval would be similar to the one described above.

4.4. Example implementation

Today, Mobile PKI has been well implemented and proven successful in many countries especially in Europe, including Finland, Estonia, Iceland, Norway, Switzerland, Turkey, Azerbaijan etc. The following section gives a brief overview of the Mobile PKI implementation in Finland.

4.4.1. Mobiilivarmenne

Mobiilivarmenne[26] (Mobile Certificate in English) is the Mobile Signature Service (MSS) implementation by the three major mobile network operators (Telia, Elisa and DNA) in Finland. It was implemented in close cooperation with the Finnish Federation for Communications and Teleinformatics (FiCom) and was commercially launched in June 2011. Mobiilivarmenne is a basic implementation of mobile signature service based on ETSI MSS standards [49], [50], [51], [52] and provides strong electronic identification and authentication for users. It is an identity service offering a shared, common platform for application providers to authenticate users, irrespective of the operator to which they are subscribed to [55], [59], [60], [61].

The main selling point of the Finnish Mobile ID implementation is its cycle of trust architecture which allows for signature "roaming" between all the MNOs in the cycle of trust. Normally, an Application provider is required to make a service agreement with all individual mobile signature service providers (MNOs) to be able to reach their users. In the Finnish Mobile ID Circle of Trust, however, there exists a cooperative framework between the three MNOs, under which they accept Mobile ID certificates created by each other, and allow signature roaming on their network. Thus, an application provider only needs to sign a service agreement with only one operator in the cycle of trust to be able to reach the mobile PKI subscribers of the three operators. This ensures that the user experience is the same, regardless of which operator they use [55], [61].

Like the Government driven e-ID card scheme, the legal framework for the Finnish mobile ID is laid down in the Finnish Act on Strong Electronic Identification and Electronic Signatures [7]. To acquire Mobiilivarmenne, a person needs to be, either a Finnish citizen or permanent resident in Finland with a valid government issued ID card or Passport. The user is also required to be a subscriber of one of the operators in the cycle of trust and sign a subscription contract for Mobile ID.

The Finnish Mobile ID is based on X.509 v3 certificates and public key infrastructure where the certificate private keys are generated and stored on the SIM/UICC card and is protected with a PIN. A user's Mobile certificate contains the user's first name, last name and Personal Electronic Identifier (SATU). In addition to aforementioned attributes, the mobile certificate could also convey other attributes including, address, age, gender, certificate validity info etc.

[26] *Mobiilivarmenne.* https://mobiilivarmenne.fi/eng/

if specifically requested by the AP, and the AP is authorized to process such information about the user [55], [60].

The Mobile ID Certificate comprises of two X.509 certificates, one for authentication (i.e. authentication certificate) and the other for signing (signature or non-repudiation certificate). The authentication and signing certificates are based on either RSA algorithm, with key length between 1024 and 2048-bit keys or ECC algorithm with 256-bit elliptic curves. For digest/hashing, SHA-256 function is commonly used. Each Key/certificate is protected by a user defined PIN. The authentication certificate is protected by an authentication PIN that is minimum 4 digits in length and the signing certificate is protected by a corresponding Signing PIN which is between 4 to 6 digits in length [55], [59].

Penetration

Today, there are over 200,000 reported active subscribers of Mobiilivarmenne, with the subscriber figures rising year on year since launch.[27] It is available for use at hundreds of online service providers including different government owned services at both national and municipal levels, banking, insurance institutions, MNO own online services, Healthcare services etc. A list of online service providers where Mobiilivarmenne could be used is available online.[28]

4.5. Use cases

Mobile PKI provides a solution for almost all the digital identity use cases including but not limited to,

Two-factor authentication: Mobile PKI provides two-factor authentication "Something you have and something you know" enable authentication for various online services. It has built-in support for LoA2 authentication, e.g. Social media login, LoA3 authentication, e.g. Company VPN access and LoA4 strong authentication e.g. login to government websites. Other applications include anonymous and pseudonymous authentications.

Consent: Mobile PKI allows two-factor transaction approval e.g. giving consent to complete a banking transaction.

Most Mobile PKI implementations include a **Non-repudiation** certificate for signing. Applications include signing legal documents, contracts etc. electronically.

4.6. Limitations

The biggest limitation to Mobile PKI implementation today is the requirement for a special PKI SIM card. In established Mobile ID markets such as Finland, Norway and Switzerland, PKI SIM cards are the norm, however in other markets, SIM cards without the required crypto processor are still the primary distributed cards as they are cheaper than PKI cards. Thus, in

[27] Mobiilivarmenne. "*Service Providers (In Finnish).*" Retrieved from: https://mobiilivarmenne.fi/palveluntarjoajille/ (Accessed 12/02/2018)
[28] Elisa. "*For service providers (In Finnish).*" Retrieved from: http://palveluovi.fi/ (Accessed 12/02/2018)

new markets, end users would likely be required to acquire new SIM cards to be able to use Mobile PKI.

Uploading or updating a Mobile PKI Applet over the air is challenging. Thus, extending applet functionality or performing security updates for SIM cards already in the hands of subscribers is therefore very limited

User experience quickly deteriorates in a poor (high latency and low speed) mobile network as RTT of signature messages could become very long making it unusable.

Solution is not universally available. A citizen can only access Mobile PKI if they are a subscriber of an MNO providing Mobile PKI service.

Chapter 5

BankID

Banks today, are important players in the realm of electronic identification and authentication. These relatively trusted entities have experience of dealing with high-value transactions which mandates that they be strongly assured of the identity of their customers. Banks must comply with several national and international laws and best practices guaranteeing the safety of their customers, preventing fraud, money laundering, terrorism financing, white-collar crime etc. [4]. The following presents the key foundations of banks becoming reliable identity providers today.

Firstly, banks are required to comply with customer due diligence standards, which means that they are obliged to identify and know their customers. Before establishing a banking relationship, the bank must verify the potential customer's identity from a reliable source, such as identity documents issued and registered by official authorities. The bank also must ascertain sufficient information on the customer's activities to confirm the origin of incoming money, and the purported use of the banking relationship. This provides a key ingredient required for strong person identification and authentication, which is the assurance that the person is who they claim to be. With due diligence compliance, banks know their customers and can reliably confirm the identity of the customer.

Secondly, anti-fraud requirements create strict requirements for the banks to authenticate their customers before authorizing a transaction. Banks, thus, must implement security procedures that comply with national or international standards to avoid unnecessary liability [4].

The topic of strong authentication has been an important issue for banks even before the rise of the Internet. For example, with Payment or Credit Cards, banks usually have to authenticate both card and cardholder, before a transaction is authorized. With the rise of online baking, the same regulations continue to apply to banking processes. Online banking history in Finland for example, can be traced back to the 1980s, even before there were other high risk services such as eGov., eHealth, social services etc. on the Internet. This was driven by a need to be closer to the customer, lower cost and enable greater volume of transactions at the same time. Nowadays, online banking volume has surpassed walk-in banking transactions.

Initially, single factor authentication using username/customer number and password combinations seemed to be sufficient for online banking. However, in the face of increasing fraud occurrences, new regulations came into place legislating the need for more secure multi-factor authentication methods for online banking. For example, in the United States of America, the Federal Financial Institutions Examination Council (FFIEC), recommended the use of Multi-factor credentials for customer authentication as far back as 2001 [70]. Similar

legislations were also enacted in Europe, culminating in the Second Payment Services Directive (PSD2) [71], which came into force at the beginning of 2018. PSD2 requires every payment service provider to implement strong customer authentication based on two or more authentication elements which are categorized as knowledge (something only the user knows, e.g. Password/PIN), possession (something only the user has, e.g. One Time Password (OTP) Token, smartcard or Phone) and inherence (something only the user is, e.g. Fingerprint).

Thus, many online banking authentication solutions were designed to comply with the strict regulations. Today, very few online banking authentication solutions are based only passwords, and most are increasingly based on authentication credentials provided by Transaction Authentication Number (TAN) lists, OTP tokens, smartcards, code generators, mobile phones, etc., in addition to the classic username/password combination. To acquire authentication credentials, a customer must visit a bank branch office, and authenticate his/her identity using an official ID document.

Today, electronic identification services offered by banks for usage on third-party services is only a natural extension of the authentication systems used for the bank's own services. Banks by default have been able to implement authentication services, such that they were effectively able to bind a particular online payment or transaction to the identity of the customer who initiated the transaction. The ability to reuse this authentication/transaction binding mechanism is what gave rise to BankID. BankID enables parties not already having a trusted relationship to establish secure communication and perform secure transactions on the Internet with the bank acting as the trusted party between its customers and service providers, providing a strong identity assertion between the customer and the third-party service [63].

By using a customer's banking credentials, BankID supports a wide range of use cases, including registration and login to third-party service providers, authorization of transactions, contract (i.e. document) signing etc. BankID is commonly delivered as a common identity framework with a common API allowing service providers to integrate their platforms with the BankID authentication infrastructure. Authentication is managed by the existing customer's bank, and no personal data are shared with the third-party service without the user's explicit consent.

5.1. Types

The electronic identification solution provided by banks is most popular in regions that have developed strong online banking infrastructure, such as many Northern European (so called Nordic) countries. To make available their identity infrastructure to other service providers, the banks had to define common APIs through which the third-party services could integrate with the banking e-ID infrastructure. This for example includes consortiums of the banks in Sweden for the bank e-ID implementation called BankID; another solution of the same name by Norwegian banking consortium and the TUPAS service defined by the Federation of Finnish Financial Services [4].

Although, the e-ID solution provided by the banks in the above-mentioned countries are referred to as BankID (TUPAS in the case of Finland), each of the solutions are mostly proprietary per country and not interoperable. For example, the solutions in Sweden and Norway, might share the same name "BankID", neither is compatible with the other. In fact, each of the countries have taken different approaches to implement their solutions. TUPAS in Finland is a non-PKI solution, while Swedish and Norwegian implementations are both PKI solutions.

5.1.1. Non-PKI BankID

This type of BankID does not use public key infrastructure, but some sort of shared secret for authenticating the customer. The bank authenticates its customers with the same bank-specific identifiers that the customer uses in the bank's own services. Bank-specific identifiers utilized includes Username/Password + PIN/TAN lists, OTP etc. The authentication process normally involves authenticating directly to the bank's online banking service which then assets the customer's identity to a requesting third-party service. A prime example of non-PKI BankID is the Finnish TUPAS [5], [64], [65] [68].

5.1.2. PKI-based BankID

There are also BankID implementations that are based on PKI, employing elements including smartcards, files (PKCS#12 format type) stored on the device storage, as well as centrally stored certificates in the bank's infrastructure. Swedish and Norwegian BankID take a different approach to the Finnish TUPAS solution in using PKI based solution. For example, the predominant solution in Norway is one where the user's private key is stored in a central secure bank system [63], [66], while in Sweden, locally stored soft certificates have found more application [67], [74]. PKI based implementations of BankID ensure that only the rightful owner of the private key has access to it. In the following sub-sections, brief descriptions of the elements used are given.

Locally stored BankID: This is a BankID solution where the certificates are stored as PKCS#12 [40] type files in the customer's computer or smartphones. The customer's key pairs are generated in the bank's central infrastructure from where they are downloaded to the customer's computer or smartphone. The private key is stored in the registry or file system location in the computer or smartphone. This is the primary form of BankID in Sweden [67], [75].[29]

Banks offering file based BankID provide software applications that enables the customer to download the key pair to their devices, ensure secure storage of the private key in the device's storage and authentication of the customer to access the stored private key for use during an authentication or signing session. The customer's BankID private key is protected with a static password or PIN known only to the user and is used for authenticating the customer before access to the private key is granted.

Centrally/bank-stored BankID: In centrally stored BankID, the customer's certificate and associated keys are stored in a central key store within the Bank's infrastructure. The key pairs for each individual customer are generated in a central key generator, which is part of the bank's infrastructure. A Hardware Security Module (HSM) is used as the central key store where the certificates and corresponding encrypted keys are stored. It is the most common form of BankID implementation in Norway [63], [66].[30]

To be able to access the encrypted keys, the customer is authenticated using bank specific identifiers which could be an SMS OTP, a PIN/TAN list, an electronic code generator, mobile app, or a smartcard. The use of the customer's authentication credential decrypts the customer's private keys and allow it to be used for e.g. authentication to third-party services [63].

---

[29] *Swedish BankID.* https://www.bankid.com/en/

[30] *Norwegian BankID.* https://www.bankid.no

Smartcard-based BankID: To improve security and level of assurance, there have also been a number of implementations using smartcards and secure elements such as the SIM/UICC card. This involves the generation and/or storage of a customer's cryptographic certificate and associated keys on a smartcard. The customer accesses the private key stored on the smartcard using a PIN known only to him/her for authentication and signing operations.

BankID on Card is a solution that has been implemented in Sweden;[31] it is based on smartcards similar to the physical e-ID card implementations surveyed in Chapter 3 of this thesis.

In Norway, they have opted for a Mobile PKI based BankID, referred to as BankID on Mobile. It was implemented as a cooperation between the banks and MNOs who provide the secure element hosting the customer's private keys.[32]

Smartcard-based BankID implementations will not be described further in this chapter, as they are forms of the solutions already surveyed in Chapters 3 and 4 of the thesis.

5.2. Service description

A typical BankID service architecture is presented in Figure 17. It shows a conceptual architecture combining the many components common to different BankID implementations. It also highlights the relationship between different stakeholders and elements involved in the BankID Infrastructure [63], [64].

[31] *This is BankID. https://www.bankid.com/en/om-bankid/detta-ar-bankid*
[32] *BankID on Mobile. https://www.bankid.no/en/about-us/services/*

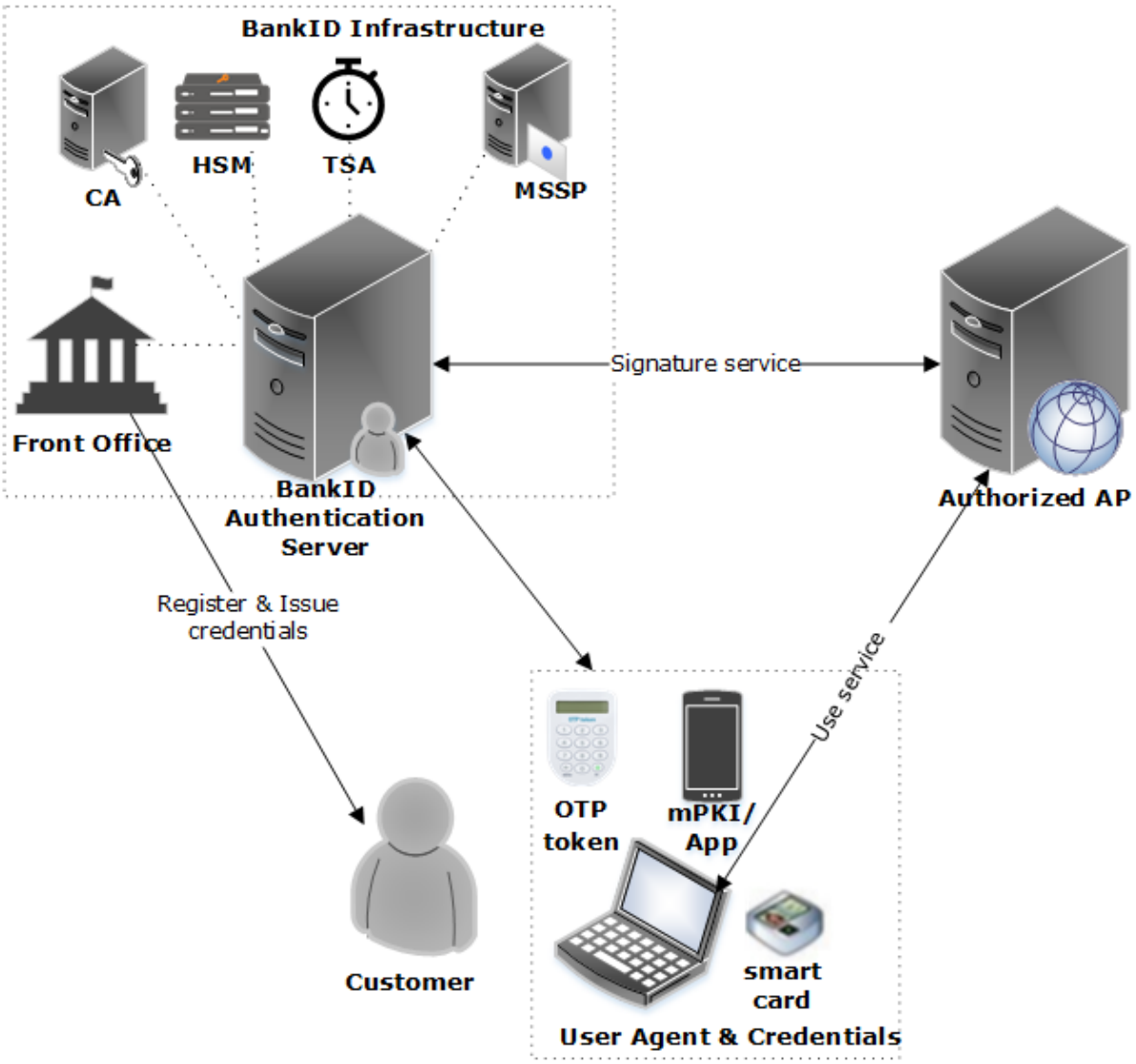

Figure 17: BankID Service architecture

5.2.1. Stakeholders / Roles

Identifying customer: The identifying customer refers to the bank's customer who uses BankID for identification, authentication or signature at a third-party service. The customer acquires the required bank specific credential for accessing the BankID service.

Authorized Application Provider: This is the Internet service provider who utilizes the BankID infrastructure to reliably identify its users. The AP signs a contract with the banks offering BankID to be able to reach the bank's customers.

Banks: The provider of the BankID infrastructure provides the primary function of certificate issuer. Banks manage the complete infrastructure, including registering a person when they become customers, issue them with authentication credentials to use with the BankID, and provide an API through which authorized service providers could use the BankID infrastructure to identify the banks customers.

The BankID infrastructure comprises of the following components depending on the kind of BankID offering:

The **Registration Authority** function is provided by the bank's front office whose function is to authenticate and verify a person's identity when they become a customer. The front office is also responsible for issuing the required authentication credential for BankID to the customer, maintaining an incident reporting service for reporting service issues, compromised credentials and requesting revocation of compromised certificate or credential.

BankID authentication server: This is the primary authentication server and concentrates the authentication and signing function of the BankID, allowing service providers and customers alike to request signature and give consent respectively. It is responsible for validating the authentication credentials of the customer and returning customer identifying information to the service provider as a response to a signature request.

Certificate Authority*:* In PKI based BankID, the infrastructure includes a CA function responsible for issuing certificates to the BankID customer. It is also responsible for revocation of compromised certificates and maintains a CRL or OCSP query service through which the validity of certificates is verified.

HSM: In Bank stored certificates; a hardware security module is used for generation of the customer's key pair, storage of the encrypted keys and corresponding certificates.

Time Stamping Authority (TSA): The TSA securely keep tracks of all signature transactions in the BankID service. This involves adding time information to the BankID signature response to the service provider, accurately depicting exactly when a transaction occurred. In a non-PKI solution like TUPAS, a time stamp helps to provide non-repudiation of the TUPAS certificate [65].

MSSP: In BankID on Mobile like the implementation in Norway, where the customer's SIM card is used for storing his/her private keys, the BankID infrastructure includes a MSSP server and gateway that allows the central authentication server to route signature requests from the Application provider to the customer's phone.

5.2.2. Service flow.

Figure 18 shows a typical authentication service flow in BankID. To be able to use the BankID service, the identifying customer must be a customer of one of the banks providing BankID and must have acquired the required credential to be able use the BankID certificate to reliably identify at the service provider. Additionally, the third-party service provider must have a service agreement with the individual customer bank (in TUPAS) or with one of the banks in the BankID consortium (in Norway and Sweden) [63], [65], [67].

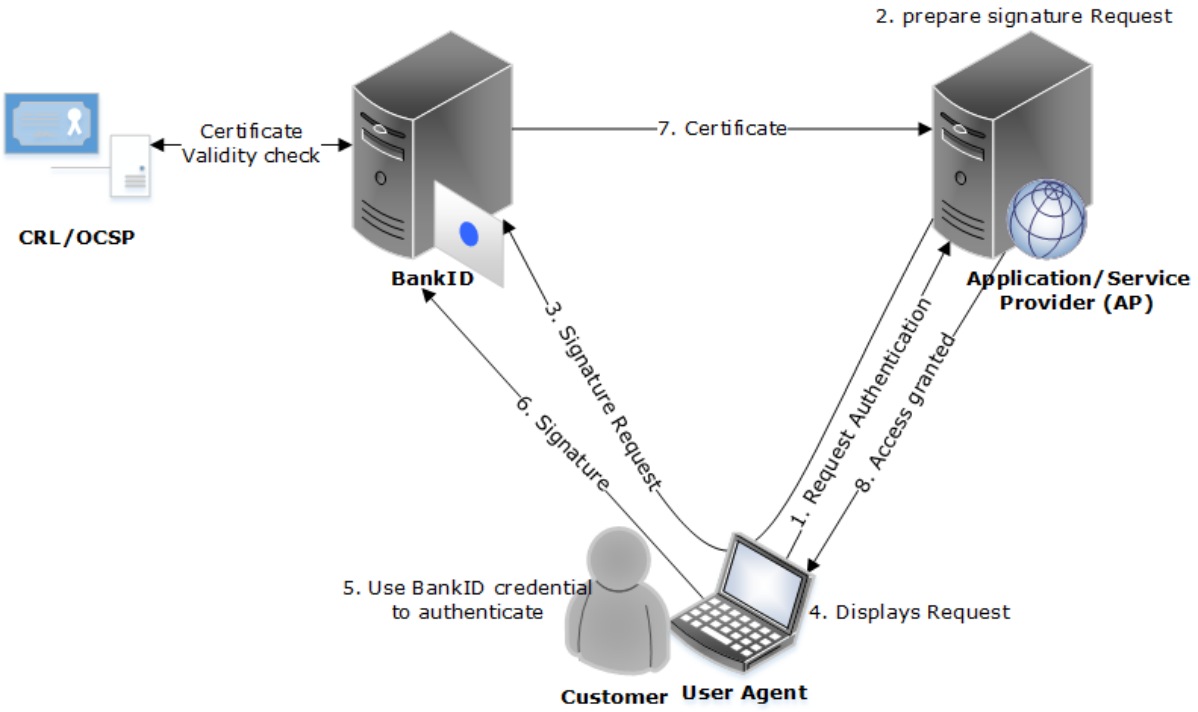

Figure 18: Authentication Service usage flow in BankID

The list below presents the service flows in TUPAS [64], Sweden's Mobile BankID (example of file/app based BankID) [75], and Norway's bank-stored BankID (example of bank-stored BankID) [63].

1. The BankID signature process begins with the customer accessing the service provider (RP) to which he/she would like to use BankID to reliably identify to.

2. The RP prepares an identification request in the required format, containing all data required by the bank to prepare a signature.

    - The customer is asked to select his/her bank in TUPAS for authentication.

    - In Sweden's BankID, if the customer has more than one BankID, he/she is asked to choose which to use. The customer selects mobile BankID application running on one of his/her devices.

    - The same way in Norwegian BankID, the customer is asked to select the BankID implementation to use (i.e. BankID or BankID on Mobile). The customer selects BankID for bank-stored BankID.

3. The RP sends a signature/identification request the BankID infrastructure or to customer's BankID client depending on the particular implementation. The bank or BankID client receives the signature request and verifies the integrity and the authenticity of the RP service.

    - In TUPAS, after the customer has selected his/her bank (see step 2), he/she is redirected to the authentication page of the bank.

- In the Swedish Mobile BankID, if the Mobile BankID selected by the customer is on the same device where the RP request was initiated, the Mobile BankID app is auto launched by the RP service. If, the Mobile BankID to be used is running on another device however, the customer is asked to provide their SSN in the RP service to route the request to the Mobile BankID app running on that device.

- In the Norwegian bank-stored BankID, a BankID client is launched within the RP service.

4. The BankID client displays the request to the user and asks if the customer would like to proceed with the transaction (or authentication) or abort.

5. The customer authenticates by entering his/her PIN or security code to authorize transmission of required attributes or certificates to the RP.

    - In TUPAS, the customer is asked to enter his/her credentials to authenticate to the online banking service. The customer enters his/her customer ID (or username) and a code from his OTP token or TAN list or PIN to a codes app running on his/her mobile device.

    - In the Swedish Mobile BankID app, the customer enters his PIN.

    - In the Norwegian bank-stored BankID, the customer is asked to enter his/her SSN, OTP and finally the static BankID password/PIN.

6. Signature Creation & Response

    - In TUPAS, the bank generates a TUPAS certificate upon successful authentication by the customer. The customer verifies the certificate's data and accepts the transmission of his/her attributes to the RP.

    - The SSN and PIN (Swedish Mobile BankID) or SSN, OTP and password (Norwegian bank-stored BankID), is used to decrypt and access the user's private keys to generate the signature response and transmit the customer's certificate and authorized attributes to the RP.

7. Certificate Return – A valid customer certificate is returned to the service provider. The RP may also verify the validity of the signature/certificate received from BankID service

8. Finally, the customer is granted access to the RP service.

5.3. Security & privacy features

Authorization: Service providers seeking to use BankID are issued with certificate or authentication keys that allow them to communicate with the BankID infrastructure. In TUPAS, the service provider uses their bank issued authentication key to generate message authentication code (MAC), which is used for encrypting the identification request sent to the bank.

Connection encryption: The data connection between the service provider, bank and customer is SSL/TLS-encrypted. This ensures end-to-end encryption of the connection, preventing man-in-the-middle vulnerabilities.

2-factor authentication: All the reviewed implementation types of BankID uses a 2-factor credential for customer authentication.

Smartcard based BankIDs using secure element like UICC cards (BankID on Mobile) or smartcards (card based BankID) offers the same high secure tamper-resistant solutions as found in Mobile PKI and national e-ID card implementations.

Access control mechanisms: The Customers completely controls the transmission and disclosure of their personal information to third party service providers. The customer must explicitly express consent before his/her data is shared with the requested service provider.

5.4. Example implementations and use cases

5.4.1. TUPAS

The BankID implementation in Finland called TUPAS is a prime example of a non-PKI based form of BankID. The TUPAS identification service allows online service providers to authenticate their customers with the TUPAS certificates issued by the TUPAS service. TUPAS is a joint bank specification for electronic authentication by the Federation of Finnish Financial Services [64], [65]. It defines the common API for integrating third-party service providers to the bank authentication infrastructure and specifies identification request and response types and message formatting. The TUPAS identification service follows the Finnish Act on Strong Electronic Identification and Electronic Signatures (617/2009) [7], which provides the legal framework for the solution [65].

Typically, banks in Finland follow regulations on Preventing Money Laundering and Terrorist Financing in carrying out the required due diligence on their customers. The banks collect information on their customers following this Act. The customer information is stored in the bank's systems and with the customer's consent, could be made available to third-party service providers for the electronic identification of the customer in their services [65]. The TUPAS identification service is available to a Finnish citizen or permanent resident with an official identification document which has been authenticated to proof the identity of the customer to a TUPAS scheme participating bank. To be able to request TUPAS certificates, the service provider must sign an individual agreement with each of the banks participating in the TUPAS scheme to be able to reach all customers [5].

TUPAS is not a qualified, PKI-based authentication solution. It is a proprietary "shared secret" identification solution using a combination of a username (or customer number) and password with one-time transaction authentication numbers (TAN) that are printed on a paper slip, generated by a code calculator token or mobile app [5]. The bank authenticates its customers with the same bank-specific credentials that the customer uses in the bank's own service. The customers identify themselves and express consent by using their bank issued credential, i.e. personal access codes or TAN lists. The customer's electronic identification confirmed by the TUPAS service is unique (usable only once) and tied to both the service provider's service transaction in question and the customer using a timestamp [65].

As TUPAS is not a PKI-based solution, there is no separate blocking list (e.g. a CRL) for the TUPAS certificates, since the certificate is uniquely created per transaction and can only be used once. The bank does maintain a blocking service for customer's authentication credentials e.g. lost TAN list, which thereafter becomes unusable with the bank's authentication [68]. The bank provides a certificate which always contains the customer's name. In addition to the customer's name, the bank may also provide the customer's social security number (HETU in Finnish) encrypted or in plaintext. Based on the TUPAS identification principles [64], a plaintext HETU should only be disclosed to service providers who have been authorized to access such data.

The primary use case of the TUPAS service is strong customer authentication. However, the TUPAS certificate could be used to create digital signatures through a process called authentication-based signing,[33] which involves the reuse of the TUPAS authentication result (certificate) for generating digital signatures. The service provider receiving the TUPAS certificate does the creation of the digital signature, and the usage of TUPAS certificate for digital signature must be mutually agreed between the service provider and the customer. Time-stamped response messages and log files support use of the TUPAS certificate for digital signatures.

Today, TUPAS is the largest strong authentication implementation in Finland used across a broad range of services including banking, e-commerce, eHealth, eGovernment services etc. Unlike the FINeID, the TUPAS service is available free of charge to customers, with only service providers paying for the service. It has been cited as the main reason why the Finnish e-ID (FINeID) card did not gain enough traction among the populace [5]. Today, it is estimated that there are around 3.5 million users of TUPAS.

In the amended law on strong electronic authentication [72], limitations were found in the compliance of TUPAS to the requirements defined in the new regulation. The regulation came into force on May 1 2017, with transitional period until September 2019, after which the TUPAS authentication service in the current form will no longer meet legal requirements for strong electronic authentication [73]. Banks have started implementing updates to the current TUPAS protocol to comply with the new regulation after the transition period.[34]

5.4.2. Swedish BankID

The Swedish BankID is a strong electronic identification solution developed by a consortium of Swedish banks, allowing reliable authentication and non-repudiation services between banks, third-party service providers, government services etc. and customers on the Internet. It is today the largest strong electronic identification solution in the country with around 7.5 million active users.[35] The Swedish BankID complies with the requirements defined for an advanced electronic signature in the EU eIDAS regulation, which today provides the legal framework for the solution.

The Swedish BankID is a PKI-based solution with user credentials available on smartcards; PKCS#12 files on a computer or BankID mobile app available for all the Mobile OS platforms.

---

[33] Signicat. "*Authentication based signing.*" Retrieved from: https://developer.signicat.com/documentation/signing/#AuthenticationBasedSigning (Accessed 05/03/2018)

[34] OP "*Authentication Forwarding Service.*" Retrieved from: https://uusi.op.fi/corporate-customers/payments-and-cash-management/merchant-services/op-authentication-forwarding-service (Accessed 05/03/2018)

[35] *This is BankID.* Retrieved from: https://www.bankid.com/en/om-bankid/detta-ar-bankid (Accessed 05/03/2018)

It is available to all persons with a Swedish social security number aged 11 or over. The core BankID infrastructure is shared by all the banks in the BankID consortium, meaning service providers only need to enter into an agreement with one bank to be able to reach customers of all the banks in the scheme [74], [75].

The customer is issued with X.509 v3 certificates that allow the customer to both authenticate and sign transactions. The primary cryptographic algorithm in use is RSA with key length at least 1024 bits. The Smartcard based BankID is valid for 5 years, while other forms of BankID (on file and on mobile) is valid for 2 years. A PIN or customer defined password accompanies the BankID which is used to authenticate and express consent for a particular signature operation [67], [74].

The primary use cases for the Swedish BankID is customer authentication and signing.

5.4.3. Norwegian BankID

A consortium of Norwegian banks provides the Norwegian BankID, giving customers the ability to authenticate and sign documents at various third party services on the Internet. It was launched in 2004, with all the participating banks sharing a Common Operational Infrastructure (COI), allowing service providers with a service agreement with one bank to be able to reach the customers of all the BankID scheme participating banks [63]. Since 2009, the BankID offering have included "BankID on Mobile" which is a Mobile PKI implementation allowing the customer's mobile device to be used as the electronic identification credential [69].

The Norwegian BankID is available to all customers of participating banks aged 13 or over. The BankID COI is closely linked to the Norwegian National Central Population Register, which contains a register of unique social security numbers of all permanent residents of Norway. Today, there are 3.7 million active users of BankID in Norway out of a total population of 5.2 million reaching over 70% of the population. Users of BankID on mobile is about 1.4 million, almost 40% of the total subscriber base.[36]

The BankID customer is issued with two different pair of keys; one for authentication and the other for digital signature. The customer's certificates are valid for a maximum of 2 years and may be auto renewed by the issuing bank before the expiry date. The primary cryptographic algorithm in use is RSA and key length at minimum is 1024 bits [66]. The BankID-issued customer certificates comply with the requirements defined for an advanced electronic signature in the EU eIDAS regulation, and thus could be used for producing electronic document signatures equivalent to handwritten signatures.

The primary use cases for the Norwegian BankID is customer authentication and digital signatures, which could be used at several authorized service providers (i.e. service providers who have entered into a service agreement with a BankID scheme participating bank).

5.5. Limitations

Malicious access to certificate: In file/app-based certificate implementations, the security of the private key depends entirely on the security of the host device. Because the certificate is stored in the device memory, there is a high risk that malicious applications on the user device (with access to the same storage and memory areas) could potentially retrieve certificate data

[36] Bankid.no *"3,785,114 Good reasons to use BankID."* Retrieved from: https://www.bankid.no/en/company/ (Accessed 27/07/2018)

or passively capture or substitute customer's keys usually without the customer noticing the attack.

Soft certificate availability across devices: Another limitation of file/app based BankID is that the usage of the customer's certificate is restricted to the user agent, meaning the customer might have to install or copy the certificates manually to all his/her devices.

No consensus on assurance of non-PKI solutions: There is an open question as to whether a non-PKI implementation of strong electronic identification meets the requirements for advanced electronic signature. LoA4 specification according to the ISO/IEC 2915 standard requires the use of tamper-resistant hardware token and cryptographic keys completely in control of the end user. Based on this definition, non-PKI implementations like TUPAS do not qualify for LoA4 electronic identification services. Also, because TUPAS is not based on electronic certificates, digital signatures for e.g. document signing cannot be easily produced.

Privacy in TUPAS: A limitation in TUPAS for example is the transfer of customer's privacy sensitive social security number (SSN) in plain text. This compromises the security of the SSN data, potentially allowing malicious programs on the customer's device or browser to read the data [73].

For centrally stored PKI solution, the primary weakness comes in the ***security of the authentication process*** that enables the end user to access the centrally stored keys. Most implementations use a combination of a password or PIN and an OTP which cannot be regarded as providing an adequate amount of security. In addition, the private key is not exclusively in the control of the customer; it is stored on a server-side HSM. The security of the private keys is solely dependent on the bank's key store practices. It is indeed safe to say that a centrally stored e-ID solution requires more complex set-up to do it right.

To implement multi-factor authentication, bank-stored solutions must implement more complex authentication schemes to support more than one authentication factor (e.g. Knowledge). This could be done through the registration of the subscriber's phone number through which they could receive an OTP or other more complicated mechanisms such as mobile app synchronized with the subscriber's device among others.

BankID is not universally available. A citizen must be a customer of a BankID providing bank to be able to use the e-ID solution.

Chapter 6

Solution assessment & comparison

The ability to securely link a set of information to a real entity (e.g. real citizen or a business entity) is essential to various critical interactions and services on the Internet. This secure link is made possible through a combination of technologies and processes that creates a strong electronic identity for an entity. This thesis in Chapters 3, 4 and 5 surveyed strong electronic identity solutions under three broad groups, namely Physical e-ID cards, Mobile PKI and BankID.

The surveyed solutions do not necessarily take the same approach in implementing the strong electronic identity. In this chapter, a brief assessment and comparison of the surveyed solutions is presented.

6.1. Criteria for comparison

A lot of factors are often considered by policy makers when choosing a strong electronic identity solution. The factors range from organizational factors such as cost and ease of implementation and use, key stakeholders, mobility and flexibility, among others and important technological questions such as the foundational technology upon which the solution is built, security and privacy of the solution, etc.

Such is the importance of these factors that they together influence the solution type, implementation method as well as the perceived success or failure of the solution in the marketplace after implementation. The following sections 6.1.1 and 6.1.2 identify criteria chosen for the comparison in this chapter.

6.1.1. Organizational comparison criteria

The following organizational comparison criteria are considered:

Key solution stakeholders: Who are the key stakeholders? This criterion assesses the solutions based on the key stakeholders involved in the provision of the e-ID solution infrastructure and service.

Cost: How much does it cost the user? I.e. how much does the user pay to acquire the solution (i.e. registration/activation)? In addition, how much does the user pay for service usage? This criterion assesses the solution based on the apparent cost of the solution to end users. The key figures used for the assessment are from the pricing practices of selected assessment examples.

Usability: How long is the validity period? In addition, how easy is it to extend/replace the certificate/credential after expiration of its validity period? This criterion assesses the solution based on the time duration during which the user can use the e-ID solution before expiry or exhaustion and the ease with which the user could either replace or extend the certificate or credential.

Mobility: Does the solution support mobility? This criterion assesses the flexibility of the solution from the view of mobility. Is the solution usable on Mobile? It also assesses the solution on whether the solution could be used on a device other than where the operation (signature request) was initiated.

6.1.2. Technological comparison criteria

The following technological and security criteria are considered:

Technology: What underlying technology is the solution based on? This criterion assesses the solutions based on the foundational technology upon which the solution is based. It seeks to differentiate the solutions as either PKI based or non-PKI based.

Use cases: What use cases does the key or credential support? This primarily defines the purpose of the key (i.e. key usage) contained in the issued end user certificate. This criterion shows what kinds of use cases are supported by the solution (e.g. electronic ID/Authentication, electronic signature).

Security token: What sort of security token is used for securing and storing user's private data or key? The standard definition of level of assurance 4 (LoA4) according to ISO/IEC 2915 (or high in eIDAS) recommend the use of a tamper-resistant hardware security token for storing the end user's private data or keys. This criterion assesses the solutions based on the kind of security tokens used in its implementation.

Key management: How are the user's keys generated and managed? This criterion assesses the solutions based on how, where and when the user's key pairs are generated and or stored.

Authentication method: What authentication factors does the user use to access their private key or express consent? This criterion assesses the solutions based on the action that the user must perform to express consent to proceed with or complete a transaction. As there are different methods available, this criterion identifies and compares the solutions based on the predominant user authentication method used.

Levels of Assurance: What level of trust/confidence can be placed in a signature produced by the solution? This criterion assesses the solutions based on the overall levels of confidence that could be gleaned from a signature or certificate produced by the solution in response to a request for identification from a third-party service.

Privacy: What privacy protecting features are built into the solution? This criterion assesses the solutions from the view of privacy, what features, or policies have been put in place in the solution that enhances the privacy end users of the solution.

6.2. Assessment examples

To simplify the solution assessment process, one assessment example for each solution type have been selected and is used as the basis of comparison. Listed below are the assessment examples chosen for each solution method.

German eID: The German eID card is the assessment example for physical e-ID card implementation of strong electronic identity. It has been chosen because it is one of the most recent implementations and makes technology choices that not only make the solution secure but also privacy protecting. It also uses a contactless smartcard chip rather than the more widely available contact card implementations.

Mobiilivarmenne: Mobiilivarmenne is the assessment example for Mobile PKI implementation of strong electronic identity. It is the brand name of the Mobile PKI implementation in Finland by the three largest MNOs (Elisa, Telia and DNA) forming the Finnish trust network. Mobiilivarmenne has been chosen as the reference solution as it is one of the first successful implementations of Mobile PKI that is driven completely by the MNOs. Each of the MNOs may have MSSPs and applets from different vendors, but all the systems work together (enabling roaming) seamlessly within the trust network

TUPAS: The only example of a non-PKI BankID surveyed in this thesis is TUPAS, which is the BankID implementation by the Federation of Finnish Financial Services. The assessment example used for comparison with the other solutions is ***Nordea bank Codes***, which is Nordea bank's implementation of TUPAS. The Nordea bank Codes include an OTP Code calculator (hardware token) or a mobile application (Nordea Codes App) available for smartphone OSes including Android and IOS which generates and sends an OTP code to the bank's authentication system after user authentication (done after correct entry of PIN). The Nordea Codes previously also included TAN lists where the OTP codes are printed on paper. The assessment considers only the Code calculator/token and the Codes app.

Sweden's Mobile BankID: The assessment example for file or mobile app based BankID Certificates is the Swedish Mobile BankID, which is a BankID implementation by a consortium of Swedish banks. The Mobile BankID is a mobile app available for smartphone OSes including Android and IOS within which the user's private key is stored. The Mobile BankID app serves as the token through which the user can access and use BankID.

Norway's Bank-stored BankID: The assessment example used for Server-side BankID certificates is the Norwegian bank-stored certificate which is one of the BankID implementations (the other being the Mobile PKI based BankID on Mobile) by a consortium of Norwegian banks. The customer's key pairs are generated and stored on the server side and typically rely on complex authentication schemes to grant access to the certificate for usage by the user.

The Assessment examples cover all the strong electronic identity solution types surveyed in the thesis and provide the opportunity for the author to easily compare the solutions within the context and boundaries of the thesis.

6.3. Assessment & comparison results

Table 1 below summarizes the assessment results based on the technological and organizational criteria for comparing the solutions. Each solution assessment example is in a separate column with one assessment criterion defined on each row. The results of the assessment examples based on each assessment criterion is presented side by side on each row to provide a clear and concise way to compare the solutions.

Following the table, some criterions are highlighted for further description.

Solution / Criteria	**Physical e-ID cards** **Assessment ex.: German eID**	**Mobile PKI** **Assessment ex.: Mobiilivarmenne**	**Finnish BankID (TUPAS)** **Assessment ex.: Nordea Bank Codes**	**BankID (file/App based Certificate)** **Assessment ex.: Sweden's Mobile BankID**	**BankID (Server-side Certificate)** **Assessment ex.: Norway's bank-stored BankID**
Key solution stakeholders	The government provides all primary functions, including RA, CA & Issuer functions for the primary e-ID function. Authorized third-party CAs issue certificate for electronic signature	Each MNO provide own RA & Issuer functions. CA function could be provided by the MNO or by a third-party CA.	The bank provides all functions i.e. RA & Credential issuer.	Each bank provides own RA & Issuer functions. CA function could be provided by the bank or by a third-party CA.	Each bank provides own RA & Issuer functions. CA function could be provided by the bank or by a third-party CA.
Technology	PKI	PKI	Non-PKI	PKI	PKI
Key Usage	By default, electronic ID. Opt-in electronic signature acquired after card issuance	Electronic ID and electronic signature	Electronic ID	Electronic ID and electronic signature	Electronic ID and electronic signature

Security Token	Physical smartcard	Enhanced (PKI) SIM card	Codes token or mobile app	Device storage	Server-side HSM & client-side OTP token
Key management	eID function keypair (non-unique) generated before card delivery. Electronic signature key pair and certificate issued on purchase from authorized CAs	Onboard Key generation i.e. Key pair generated in the SIM card during user activation.	OTP used. No PKI key pair generated or used.	Key pair generated when user order BankID. Key pair is downloaded & paired to Mobile BankID app on user device.	Keys are generated in central bank infrastructure and stored in HSM.
User Authentication	2 factor Authentication: – Possession (e-ID card), and – Knowledge (PIN)	2 factor Authentication: – Possession (Mobile phone), and – Knowledge (PIN)	2 factor Authentication: – Possession (Code token/app), and – Knowledge (PIN/OTP)	2 factor Authentication: – Possession (Mobile device), and – Knowledge (PIN only[1] or SSN + PIN[2]) or – Inherence (fingerprint or facial scan) [3]	2 factor Authentication: – Possession (OTP token), and – Knowledge (SSN + OTP + Password)
Levels of Assurance	LoA4 – LoA4 Identity assurance – LoA4 authentication assurance	LoA4 – LoA4 Identity assurance – LoA4 authentication assurance	LoA3 – LoA4 Identity assurance – LoA3 authentication assurance	LoA3 – LoA4 Identity assurance – LoA3 authentication assurance	LoA3 – LoA4 Identity assurance – LoA3 authentication assurance
Privacy	Privacy-protecting ABCs (i.e. no X.509 certificate) used in e-ID function.	Privacy protecting policies available via on signature profiles.	TUPAS always returns all user attributes to requesting RP.	BankID always returns all user attributes to requesting RP.	Some form of privacy protecting policies implemented.

Mobility	eID cards could be read by NFC enabled phones. Can only be used on the device where operation was initiated.	SE is the SIM card, so usable on Mobile. User can initiate operation from his/her mobile phone or other device	OTP token or Mobile application. User can initiate operation from his/her mobile phone or other device	Token is Mobile application. User can initiate operation from his/her mobile phone or other device.	Token is server-side HSM + OTP token. User can initiate operation from his/her mobile phone or other device**.**
Cost	Starting from 22€ to acquire e-ID card. 0€ service cost Users must purchase separately X.509 signature certificates from authorized CAs to use signature function. Users might have to acquire card reader device	0€ to acquire 1 – 2€ monthly service fee depending on user's MNO. No need to acquire extra device	No fees to acquire or use No need to acquire extra device, as the credential is available free of charge from the bank.	No fees to acquire or use No need to acquire extra device	No fees to acquire or use. There might be some fees to acquire the OTP token, depending on the BankID issuing bank.
Usability	Card valid for 6 - 10 years. Holder must acquire new card on expiry	Certificate valid for 5 years and can be auto renewed to continue service	Certificate generated per transaction. Codes do not run out.	Certificate valid for 2 years and can be auto renewed to continue service	Certificate valid for 2 years and can be auto renewed to continue service

Table 1: Strong e-ID example implementations: assessment & comparison results

[1]*If the Mobile BankID app is installed on the same device used to initiate service (e.g. user's Phone), only user's PIN is required*

[2]*If user initiates service from another device (e.g. a computer), he/she must provide their SSN on the computer and enter the PIN in the Mobile BankID app to express consent.*

[3]*Inherence factor support is available only for authentication.*

The key stakeholders of most strong electronic identity solutions could be public or private enterprises and, in some cases, a result of a partnership between public and private entities. Of the assessment examples considered for comparison, only the German eID is issued by a government entity, the rest are issued by private entities such as banks or MNOs. However, in each of the solutions, the government or its agencies are involved in one way or the other e.g. through regulations and standardization of the solutions.

All the assessed solutions other than TUPAS are based on PKI. TUPAS is based on OTP and therefore supports only the e-ID function (i.e. authentication) by design. The Norwegian bank-stored Bank-ID, although uses PKI technology for creating digital signatures for transactions, authentication of the user (to get access to the private key) is based on OTP. All PKI based implementations (including the Norwegian bank-stored BankID) support both e-ID and electronic signature functions. The German eID implementation unlike the other PKI based solutions does not use X.509 certificates for the e-ID function; it makes use of Attributes based Credentials (ABCs). ABCs are a privacy protecting electronic identity mechanism which rather than return unique person identifying X.509 certificates to a requesting application returns only the person attributes expressly authorized by the user along with a non-unique signature; this prevents the identification of a user from a certificate except an authentication has been successfully completed by that user. Like the other PKI based solutions implementations, it does use X.509 certificates for the electronic signature function.

TUPAS does not have any privacy-protecting feature built into the solution; it always returns all user attributes including the SSN. The Swedish Mobile BankID like TUPAS also returns all information stored about the user, including the user's SSN to the requesting party along with the X.509 certificate. Although, it is possible for some of the information to be stripped off by an IDP (if the RP is requesting service through the IDP), this relies solely on the IDP to implement such privacy policy.

Mobiilivarmenne on the other hand, makes use of the concept of authorization levels for each RP and signature profiles included in each signature request to determine what is included in a signature response. For example, a RP requesting for an anonymous authentication (indicated in the SignatureProfile), e.g. to proof that the user is an adult, never receives the user's certificate and gets only true/false Boolean etc. In that way, Mobiilivarmenne ensures some form of privacy and what types of user attributes a RP is given in a signature response. Privacy is ensured in the bank-stored certificate by not including person attributes such as the SSN or user account number in the user's X.509 certificate. Instead, these attributes are kept in a Validation Authority (VA), which ensures that only authorized RPs could access the attributes. Other attributes in the X.509 certificate subject field are available to be read in the signature response returned to the RP.

All assessment examples surveyed implement at least a 2-factor authentication, based on possession and knowledge or inherence factors. Each implements the solution using a form of secure hardware token (e.g. SIM cards, OTP tokens, HSM and physical smartcard), except for the Swedish Mobile BankID which uses the mobile device storage to hold the end user's private key. All assessment examples are also available for use on mobile devices with varying degrees of flexibility. Some examples like the German eID card can only be used on the same device (computer or NFC enabled mobile device) from where the transaction was initiated at a time, while all other assessment examples can be used on a device other than where the transaction was originated.

The German eID like other e-ID card implementations offered by different governments around the world is the most expensive to acquire among the assessment examples considered. BankID assessment examples are the cheapest to acquire and use, costing nothing to acquire and use in most cases. Depending on the issuing bank, some banks might charge their customers a few euros to acquire the hardware OTP token used for authentication to the BankID systems. Mobiilivarmenne like BankID also does not cost money to acquire but MNO charges some monthly service subscription fees. In terms of cost, BankID implementations are the cheapest to acquire, use and renew for end users.

All assessment examples comply with the highest level of identity assurance by implementing face-to-face enrollment of users before service activation. In cases where a remote (or online enrollment) is supported, the user is first authenticated using another strong electronic identity solution. This is possible through "trust", where the strong e-ID solution being acquired by the user trusts that the strong authentication solution had previously verified the user's identity through a standard and trusted enrollment process. For example, a user with FINeID card could be strongly authenticated online with his/her e-ID card to enroll and acquire Mobiilivarmenne without the need to go through the face-to-face registration process. This is because the user's identity had been verified and authenticated through a face-to-face registration when he/she acquired the e-ID card.

In conclusion, TUPAS, the Swedish Mobile BankID and the Norwegian bank-stored BankID, based on the assessment conducted and a strict adherence to the definitions of strong electronic identity and ISO 29115 definitions of levels of assurance, are adjudged to be equivalent to a LoA3 (or substantial LoA in eIDAS) with minimal risk levels. This is because (1) TUPAS is based on OTP and not PKI, (2) the Swedish Mobile BankID relies on the device storage for storage of the user's private key, which could potentially open it to access by malicious applications on the device, and (3) The Norwegian bank-stored BankID relies on an authentication method based on passwords and OTP codes. Due to the authentication method being LoA3, the signature produced by the process cannot then be LoA4 irrespective of the underlying technology.

Adjudged to comply with the requirements of a LoA4 solution, are the German eID and Mobiilivarmenne. The usage of ABCs and/or X.509 certificates and tamper-resistant security tokens: physical e-ID cards and SIM cards, allows for cryptographically strong electronic identification of a person, and therefore, are adjudged to offer better solutions for providing strong, non-repudiable identification on the Internet. It should be noted, however, that the actual application of levels of assurance specification for a solution depends on the country where the solution is deployed and a strict adherence to definitions by e.g. the ISO 29115 is not always followed. A country, due to various reasons might designate a LoA3 solution (according to ISO 29115 levels) as LoA4 and accepts the usage of the solution for transactions requiring LoA4 or High levels of assurance.

Chapter 7

Scenario planning & analysis of strong electronic identity

Scenario analysis according to Wikipedia[37] is a process of analysing possible future events by considering alternative possible outcomes. These alternative possible outcomes are influenced by a series of factors referred to as key *trends* and *uncertainties* in the business domain of interest. It does not seek to present an exact picture of the future, but rather is a means of projecting several observable alternative future outcomes based on identifiable trends (possible developments) and uncertainties (possible turning points).

According to Schoemaker [12], Scenario planning is a discipline, which by exploring interrelationships among basic trends and uncertainties related to a specific business domain, seeks to understand how the future may pan out. He described further that, Scenario planning as a disciplined method has been greatly applied to a wide range of issues by companies to imagine possible futures. Scenarios themselves were described as a focused approach to describe fundamentally different futures, with each scenario telling a story of how various elements might interact under certain conditions.

Key trends are referred to as important factors whose consequences are unfolding, are certain or very likely to unfold with significant impact on the future, while key uncertainties are referred to as important factors whose outcomes or impact on the future are uncertain or unpredictable.

A careful identification of basic trends and uncertainties affecting the case topic of this thesis is done to construct a series of scenarios that will help to understand the possible outcomes or direction in the future. In this chapter, scenario planning and analysis methods are used to contemplate and better understand the possible futures of strong electronic identification on the Internet. It is used as a tool for imagining and how the future might unfold.

[37] Wikipedia. “Scenario analysis.”

7.1. Scenario construction process

This section describes the processes used for the scenario planning and analysis conducted in this chapter. It describes briefly the processes followed to construct the scenarios. Quantitative modelling processes were not considered or used in constructing the scenarios.

Firstly, the time frame, scope and the major stakeholders of strong electronic identification are identified and presented.

Secondly, relevant trends covering political/regulatory, economic/business, social and technological domains in strong electronic identification are identified and examined. Thereafter, key uncertainties are also identified and examined.

Interrelationships between the key trends and uncertainties are reviewed to construct initial scenarios, which were further reviewed to construct the internally consistent and plausible scenarios that are finally presented in section 7.5.

The input for the scenario analysis were gathered from literature review, and discussion with industry experts and stakeholders.

Literature review: The study of literature formed an important information resource for the scenario analysis. The author engaged in careful study of expert and industry opinion reports and white papers to identify what are the trends and uncertainties that could be found in strong electronic identification.

Expert discussions: The author also engaged in discussions with expert players in the field of electronic identity from Methics Oy (pioneering player in MSS solutions), smartcard vendors, MNOs, Certificate issuers and electronic identity regulators over several months from late 2017 through the summer of 2018. Many trends and uncertainties were identified through these discussions.

7.2. Scope, time frame and stakeholders

The focus of the scenario planning is to find out the future scenarios in strong electronic identification.

For the government and online service providers, strong citizen/customer authentication has never been a more pressing issue. Important stakeholders that have been identified include: governments, international technology standardization and regulatory bodies, Online service providers, Device domain players including Device vendors, Original Equipment Manufacturers (OEMs) and platforms (e.g. IOS, Android, KaiOS), strong electronic identity providers including governments, MNOs and banks and finally the end users (citizen or user or customer).

Given that the Internet today is mostly without borders, the scope for the scenario planning is worldwide, but has been limited to strong electronic identity solutions that support the highest levels of assurance (i.e. LoA4). This thesis looks at what is likely to happen in strong electronic

identity and how existing and new solutions and technologies will evolve over a period of twelve (12) years to 2030.

7.3. Key trends

Key trends in the context of the subject area (strong electronic identification) are important unfolding events and factors that are certain or very likely to occur, which will have significant impact on the future. Several trends encompassing political/regulatory, economic/business, social and technological domains were identified and examined from research and literature studies as well as expert discussions. The final key trends were created from a combination of several trends and have been condensed so that only the most important trends, which underlie the constructed scenarios, are presented below.

1. **Increasing global connectivity**

The increasing proliferation of cheap mobile devices globally and rapidly expanding broadband coverage is driving a rapid increase in the number of people connected globally. According to the Ericsson Mobility Report [48] published in June 2018, it was estimated that there were more than 5 billion unique mobile subscribers at the end of 2017. Mobile-broadband subscriptions were estimated to be around 4.3 billion globally at the end 2017. And according to ITU's ICT Facts and Figures for 2017, 70% of the young (15 to 24-year olds) and 48% of the world's total population are already connected and using the Internet [78]. The proportion of the population using the Internet in Finland like other developed countries is even higher at 100% and 88% respectively in 2017 according to statistics Finland.[38] The affordability of Internet capable devices and access to broadband is expected to continue, with smartphone subscriptions projected to reach 7.2 billion and mobile broadband coverage to exceed 95% of the global population by 2023 [48].

2. **Increasing proliferation of digital services**

The society especially in the developed world is increasingly dependent on the Internet. In recent years, there has been a concrete shift to providing services online by governments and private entities alike. Governments and private enterprises around the world seem to have realized that the transition to digital services promises significant benefits in efficiency, cost reductions, reach and easy access to their citizens or markets. Today, education, citizens' services, banking and payment services, commerce, healthcare etc. are some of the many applications that could be accessed on the Internet.

In addition, as globalization continue, countries depend more and more on each other, and more trade is being conducted digitally without physical border limitations. With more globalization come people, goods, and services that are internationally mobile, communicating and

[38] Official Statistics of Finland (OSF). "Use of information and communications technology by individuals [e-publication]." ISSN=2341-8710. Statistics Finland November 22, 2017 Retrieved from: http://www.stat.fi/til/sutivi/2017/13/sutivi_2017_13_2017-11-22_tie_001_en.html (Accessed: 29.7.2018).

transacting over the Internet without borders. Initiatives such as e-Estonia[39], the EU's single digital market are successful examples that continue to encourage increased adoption of digital services.

3. Increasing importance of identification whether online or offline

The correct identification of persons be it online or offline enable people's participation in the socioeconomic activities of a society. It has been stated that to achieve a more inclusive development in the world, a sustained effort must be put into ensuring that every person in the world has an officially issued identity [3]. The importance of identification is reflected in goal 16.9 of the Sustainable Development Goals (SDGs) adopted by all United Nations member states in September 2015. The countries made a global commitment to "provide legal identity for all" by 2030 [3], [77], [81], [82].

4. **Increasing introduction of national identity programs**

Rising from the SDGs, we are seeing a lot more countries over the last few years introduce countrywide or national identity programs. Today there are many ongoing initiatives such as the World Bank's Identity for Development (ID4D)[40], ID2020[41] among others, are helping countries without an established official identity program available to all their citizens to finance and introduce such programs.

In an ITU-T review of National Identity Programs in some 43 developing countries in 2016, it found that 29 of the reviewed countries had introduced national identity programs in the decade to 2016, while 14 others had introduced such program in 5 years to 2016. These range from very successful cases for example in India, Pakistan and Uganda, to more promising cases such as in Nigeria, Thailand, Ghana etc. There is a clear trend of governments introducing national identity programs across the world today [78].

The introduction of national identity programs is very promising as having an official identity document is a primary requirement for acquiring a digital identity. This therefore will provide a boost for e-ID adoption and implementations around the world, with at least 136 countries expected to have national e-ID programs by 2021 according to an Acuity Market Intelligence.[42]

5. Mobile is transforming the world.

The popularity of mobile devices in today's world cannot be overemphasized. Mobile devices and connectivity have become almost ubiquitous, with almost 70% of the global population owning a mobile phone [48]. In the last decade, mobile service usage has evolved from predominantly voice and short messages to include several other applications. As mobile

[39] e-Estonia. https://e-estonia.com/

[40] http://id4d.worldbank.org

[41] https://id2020.org/

[42] Acuity Market Intelligence. *"The Global National eID Industry Report: 2017 Edition."* Retrieved from: https://www.acuity-mi.com/GNeID_Report_2017.php (Accessed 29/07/2018)

devices become ubiquitous, there is an increasing demand for new use cases especially in payments and identification.

A common theme for Internet applications today is what is called a "mobile first approach", where various entities are designing their service first for mobile environments. Prominent among these applications are financial (digital) transactions, for which mobile phones are increasingly becoming the device of choice. These range from the simple USSD implementations of mobile money in East Africa,[43] to mobile payment services from large Internet companies like Apple, Google, Alibaba, Samsung, among others.

Mobile devices are also becoming important tools used in identification. Today, some of the most successful implementations of strong electronic identity for citizens have been on mobile, with examples such as BankID on Mobile in Norway, Mobiil-ID in Estonia, Mobiilivarmenne in Finland to mention a few. Other examples of mobile application in identification, include, helping with birth registration in countries like Tanzania and Pakistan [25], [81], [82], implement possession-based or inherence-based strong authentication, digitize government issued cards such as the driver's license with examples from countries including Netherlands, United States, Austria and Finland. Other countries such as China are using mobile apps to digitize their national ID cards, allowing citizens to access digitized version of their physical e-ID cards through their smartphones.[44]

6. **Increasing online fraud**

According to the Javelin Strategy & Research report, customer information breach has been suffered by as many as 1 in 3 businesses in the United States and between 2015 and 2016, online fraud related to the financial services industry affected 1.4 million consumers resulting in a whopping $2.3 billion in losses, an increase of 64% from 2015 [83]. The use of passwords and the inherent weak identity verification contribute to a majority of these fraud cases. In recent years, companies such as Yahoo, Equifax, LinkedIn, Experian, among many others have suffered damaging data breaches. The data breaches especially when user credentials are stolen could proof even more devasting as users have been found to reuse the same passwords across online services. Once a customer record from one online service is stolen, cyber criminals attempt to use this information also facilitate fraud on other services.

With the increasing profitability of cybercrime, no wonder the trend has continued, with Gemalto reporting in their Breach Level Index report for 2017 that as much as 2,600,968,280 records were breached in 2017. Identity theft and financial access accounted for 84 percent of all breaches, both seeing significant increases from 2016 with 73 and 189.1 percent respectively [84].

[43] Wikipedia. *"M-Pesa."* Retrieved from: https://en.wikipedia.org/wiki/M-Pesa (Accessed 02/08/2018)
[44] Li Tao. *"A look at China's push for digital national ID cards."* South China Morning Post, January 23, 2018. Retrieved from: https://www.scmp.com/tech/article/2129957/look-chinas-push-national-digital-id-cards (Accessed 26/07/2018)

7. **Increasing standardization of electronic signatures as legally binding.**

Across the world today, electronic/digital signatures produced by strong electronic identity solutions are legally binding for various business and personal transactions. The EU's eIDAS regulation is in part intended to standardize the use and acceptance of electronic signatures across the EU. Many countries around the world have also enacted own electronic signature laws including Australia, Canada, Japan, Russia, Singapore, South Africa, Switzerland, United States, etc. or have ratified the UN's Electronic Communications Convention (ECC) and recognize electronic signatures as legally binding signatures.[45]

8. **Increasing demand for strong electronic identity as more high risk services take up the Internet as a vehicle to deliver services.**

A primary requirement to access digital services such as online banking and citizen services is a strong authentication means. In fact, virtually all interactions or transactions carried out online today require some type of digital identity. In the globalized and connected world of today, the need to strongly identify and authenticate people, protect personal data, prevent fraud as well as the low level of assurance that could be placed in password authentication, will continue to drive states, businesses, and individuals themselves to demand for strong electronic identification and authentication solutions for the Internet.

9. **Increasing benefits from trusted electronic identity**

The benefits of strong electronic identity cannot be over emphasized. In countries where there has been successful implementation of e-ID solutions, have all seen uptick in possibilities for government to expand its e-government infrastructure to deliver services faster and reach more of its citizens. A joint analysis report by the Secure Identity Alliance (SIA) Boston Consulting Group in 2014 indicates that trusted digital identity will generate gains in efficiency and convenience worth up to $50 billion per year by 2020 in global savings [79]. The same positive effect is also felt by enterprises who can conduct businesses and enter into agreement with the government, other enterprises and customers quickly and remotely. The e-Estonia project is a good example of the transformative benefits that strong electronic identity brings in reducing bureaucracy and facilitating efficiency. Similar eGovernment initiatives are being driven by strong electronic identity programs in many other countries around the world [25], [79].

10. **Stricter regulations regarding privacy and data security**

Before now, online services have been freely gathering huge data on their users, both that are relevant for the user's applications and many that are not, both with and without the consent of users. User on the other hand seem to offer their data to all and any service without knowing for what purposes it will be used. The increasing number of data breaches, collection, processing and transfer of user data without their consent and amid reports of some countries using such data to influence the internal policies of other countries have prompted outrage and action from governments in recent months and years. Foremost among these regulations with

[45] Wikipedia. *"Electronic signature"* Retrieved from: https://en.wikipedia.org/wiki/Electronic_signature (Accessed 27/07/2018)

wide ranging impact on how companies collect, process, share and store data can be found in Europe with the general data protection regulation (GDPR) of the EU. GDPR seeks to improve the security and privacy of personal data in the EU and requires that the control of personal data rest with the individual, with fines of up to 4% of global annual revenue for noncompliance. It is argued that putting more power in the hands of users and more transparency, will go a long way in reducing unease about adopting electronic identities.

7.4. Key uncertainties

Key uncertainties in the context of the subject area (strong electronic identification), are important factors whose direction and impact on the future cannot ascertained. They are ambivalent factors whose impact could lead to alternate futures. Key uncertainties like key trends seek to provide a stable ground upon which scenarios are built by presenting pessimistic and other less probable factors or occurrences for consideration by the scenario construction process to produce balanced and plausible scenarios. The key uncertainties are presented below.

1. **Privacy and trust**

This uncertainty seeks to present views on how trust among end users could produce alternative outcomes for strong electronic identity. Identity systems as the name and function implies, collect identifying information about citizens. In addition to the already collected and stored identifying information, it also has the potential to aggregate large amounts of data on citizens through the collection and monitoring of credential usage for various transactions on the Internet. The collection of transaction details is required for auditing purposes and to ensure non-repudiation. This raises privacy risks that totalitarian regimes could use e-IDs as a means of tracking the life of their citizens online.

Such privacy risk is nothing new. George Orwell is his book "1984" cautioned "Big Brother is Watching You!", arguing that centralized ID systems could represent the start of a slippery slope to greater surveillance and monitoring of citizens [87]. The requirement by some governments around the world that their citizens use the government issued strong e-ID with all online services brings credible fears to light. In fact, in many countries today, the rapid expansion of electronic identity systems is seen as a big threat to the freedom, privacy and security of personal information. This has served as a cautionary tale that is not lost on people and has influenced resistance to national electronic identity introduction for a long time in many countries

Likewise, in this era, where data is currency, how does the user trust that their electronic identity provider would not sell their aggregated transaction data for profit? It is not uncommon for personal information of people held by providers to be sold for purposes such as direct advertising etc. The Finnish Population Register Centre, issuer of the FINeID according to its website[46] sells the personal data it holds for direct advertising, market research, opinion polls,

[46] VRK. *"Privacy protection is essential."* Retrieved from: https://vrk.fi/en/privacy-protection (Accessed 30/07/2018)

public registers or genealogical research except a citizen explicitly forbid such disclosure.[47] Although, there are no public data on similar practices by other providers reviewed in this thesis, it is not unexpected that they could be doing the same.

The key question is, would citizen's trust in their government to not surveil their online lives be strong enough to encourage adoption of solutions provided by governments or will citizens trust the private market solutions more to adopt their solutions instead? Trust in governments and entities such as MNOs and banks is relatively high in Nordic countries which may inform the reason why electronic identity solutions have been very successful in the region. On a global scale, the trust that citizens have in their government, MNOs, banks and other e-ID providers will influence the development and success of strong e-ID solutions in the future.

2. Emerging and advancing technologies

There are several research efforts dedicated at providing suitable technological solutions for strong electronic identity that is suited for the 21st century global Internet.

Prime among these are Biometrics based authentication technologies, the maturity of which will drive new approaches for implementing strong electronic identity solutions. The massive deployment of biometrics as the primary authentication solution on smartphones from the largest vendors such as Apple, Samsung, Huawei, Sony etc., show that the biometric-based authentication revolution is here. Although, there is already a wide acceptance of biometric authentication such as fingerprint scanning and facial recognition on smartphones, how much of an influence it will have on the technology, regulatory and policy choices made by governments, policy makers and strong electronic identity issuers is not certain at this point.

Another technological advancement that could lead to alternative strong electronic identity future is Trusted Execution Environments (TEE) [85], [86]. [48] A TEE combines a hardware platform and its own trusted operating system to provide a secure and tamper-resistant environment for hosting Trusted Applications (TAs). The TAs are isolated from applications in the device main operating system, i.e. the so-called Rich Execution Environment or REE. With features including support for strong cryptography, secure storage, and a trusted user interface for secure user interactions, TEE includes all the features that would make it an excellent technology for delivering strong electronic identities. There is already support for TEE on major chips and device platforms but there are no matured TEE application as of yet. Although, the promise of TEE for strong electronic identity implementation is real, how the technology advances, pace of maturity, and what impact it would have cannot be ascertained at this point.

---

[47] Yle News. *"Report: New EU data directive won't prevent Finnish agencies from selling personal data."* 9.4.2018 Retrieved from: https://yle.fi/uutiset/osasto/news/report_new_eu_data_directive_wont_prevent_finnish_agencies_from_selling_personal_data/10150955 (Accessed 26/07/2018)

[48] Wikipedia. *"Trusted execution environment."* Retrieved from: https://en.wikipedia.org/wiki/Trusted_execution_environment (Accessed 26/07/2018)

New emerging technologies such as blockchain could also affect how we design, implement and manage identities in the future. Initiatives such as the aforementioned ID2020, seek to use the immutable feature of blockchains with biometrics to provide secure, verifiable, and persistent electronic identities. How much of a real impact blockchain will have on electronic identity at this point is debatable.

Other technological advances in cryptography, signature algorithms and their perceived security, mobile device platform security, embedded secure elements (eSEs), embedded UICCs (eUICCs), among many others could influence the complete infrastructure upon which strong electronic identity is built, bring in new players such as device vendors, and the dominating credentials or technologies used in strong electronic identity implementations.

3. **End of government monopoly on strong electronic identity?**

The strong identification of citizens has been the purview of government authorities for most of civilization. Primarily in the physical world, the government remains the official source of identity. With strict know-your-customer (KYC) requirements imposed on private enterprises such as mandatory SIM card registration by MNOs and strict KYC obligations for banks, these private entities could seek to leverage their deep KYC and assets to provide strong electronic identity, decoupling the provision of such solutions from the government. The question whether governments will relinquish their dominant role on the issuance of all citizen identities and allow private entities to become primary issuers of strong electronic identity remains to be seen.

4. **Technology standardization**

Standardization is a key ingredient for success in the development of any new technology. Technology standard influence the design of strong electronic identity systems and overall approach taken by solution providers. As we have seen with many technologies over the years, an open standard technology encourages quick large-scale deployment over proprietary technologies that are not based on open standards. Incompatible standards e.g. for signature algorithms could mean that interoperability of solutions is impossible to achieve. What sort of open technology standards for strong electronic identity would come onto the scene and their particular influence cannot be ascertained at this point in time.

5. **Interoperability of strong electronic identity solutions**

International and governmental regulatory policies determine the technical specifications, and processes followed in the implementation of the strong electronic identity solutions, as well as define the obligations of solution providers and other stakeholders under the law. These policies also specify if the implemented solutions constitute legally binding signatures. The true value of strong electronic identification can only be fully realized when there are similar regulatory policies for strong electronic identification across the globe.

The European Union set the pace with projects such as Secure Identity Across Borders Linked (STORK) and today defines a common framework for strong electronic identity solutions in the EU under the eIDAS regulation, promoting interoperability of solutions implemented in

different member states. Unfortunately, many countries lack clear interoperability and legislative frameworks for strong electronic identity solutions. How regulatory policies evolve across the world will influence the maturity of electronic identity solutions, and what solution types become widely accepted.

6. **Levels of Assurance assessment**

In response to advances in technology, levels of assurance assessment standards will be redefined. Whether this will allow for new implementation technologies and/or solution types to be recognized as providing strong electronic identities remains to be seen.

7. **Costs**

It goes without saying that implementing strong electronic identity solutions is not without costs. This costs and effort required is even greater for markets without matured identity programs for the physical world. Cost will arise from implementing the information infrastructure, procuring and issuing citizen credentials, operating and managing all the functions required to deliver a working service. Will the attending costs reduce or increase in the future and how its impact on return on investment will influence which stakeholders and how many get into the business remains to the seen.

8. **Chicken & Egg problem**

How will the chicken & egg problem affect investments and adoption of strong electronic identity solutions? Will citizens adopt electronic identities based on its promise, which will drive more online service providers to integrate the solutions on their platforms or will issues of surveillance, privacy and trust issues deter users? Will regulations and standardization drive more services to integrate with strong e-ID solutions, which will in turn drive user adoption; or this strategy, would fail completely? The chicken & egg problem will invariably influence the value, effectiveness, trust and overall buy in to the promise of e-ID from citizens and service providers.

7.5. Scenarios for strong electronic identity

The final scenarios presented in this section were constructed from a series of initial scenarios constructed from the key trends and uncertainties presented in sections 7.3 and 7.4 and checked for consistency and plausibility. The three scenarios presented help to understand what combinations of factors are influential to alternative outcomes and are named descriptively to clearly convey what alternate future they present. An alternate future devoid of strong electronic identities is considered infeasible

The resulting scenarios should not be treated as forecasts but rather as means for contemplating and understanding what future uncertainties may hold.

1. Physical e-ID cards dominate

Physical e-ID cards will continue to be the go-to solutions for countries implementing strong e-IDs for their citizens. The possibility to use the cards in both in the physical and online worlds will continue to appeal to a lot of governments and citizens alike. In the physical e-ID card dominant future, a multitude of applications beyond just strong electronic identity will be offered on a single physical card. This will be as a result of convergence, in which the different cards currently issued by governments (e.g. driver licenses, social issuance cards, Health cards, Identity cards, travel cards, Voter's cards etc.) will all converge into a single card with the different functions available as applications or applets from the same card.

Governments will therefore continue to issue physical cards due to their versatility and their many use cases will encourage greater adoption by both citizens and application providers while diminishing the adoption of other competing solutions solving the hypothetical chicken and egg problem in favour of physical e-ID cards. The limitations facing physical e-ID cards such as the need for readers and usability on mobile devices will be eliminated. Firstly, through RFID technologies such as NFC which will be openly available on mass-market devices and secondly, contactless cards will become the industry standard for physical cards. Citizens will therefore, be able to use their cards with smartphones, tablets, computers and other smart consumer devices.

Governments will retain monopoly over the issuance of identity in both physical and online worlds. In some countries, the government will achieve this through transparency, which will lead to more trust in the government and reduce the fears of a surveillance state; while in some other countries, government policies will mandate the possession and use of only the government issued e-ID cards. In both cases, the government through various policies, will offer a solution that is more attractive to the citizen and will limit the ability of new players to emerge or compete with the government issued physical e-ID card for the provision of strong electronic identity to the citizen.

2. Mobile PKI rule

Given the associated costs in procuring cryptographic cards required for implementing strong electronic identification based on physical e-ID cards to the government, privacy and trust issues in the government, as well as usability will make physical e-ID cards unattractive to citizens and will thus, discourage adoption and usage. Most governments around the world will therefore seek to outsource the provision of strong electronic identity solutions to private entities and will provide regulations that will lead to an open market competition among providers. Government will remain the main source of official physical world identity and therefore government issued documents such as passports, driver's licenses etc. will continue to be the foundation for strong electronic identity.

Mobile PKI dominates the market with Mobile Network Operators (MNOs) holding a strong position in the issuance of strong electronic identity. The opportunity of strong identity assertion as a new source of revenue generation will drive MNO investment and introduction

of Mobile PKI based strong electronic identity solutions will become the next strategic service provided by operators.

The Universal integrated circuit card (UICC or SIM card as more commonly known) will remain the most pervasive smartcard device, available to the largest segment of the world's population. Mobile operators to comply with regulations, will know their customers and will leverage both their knowledge of the customer and the presence of the tamper-resistant UICC cards to become dominant providers of strong electronic identity. The tamper-resistant UICC card will be largely embedded inside every mobile device (i.e. eUICC/eSIM) in most markets and the few remaining markets with physical UICC/SIM card modules will be dominated by cards capable of performing cryptographic operations (so-called PKI cards).

The GSM Association (GSMA) have come to realise that mobile identity provides another frontier for profitability and with more 800 operator members spread across the globe, will use its unique position, and share clout to push global open standards and interoperability frameworks to deliver a truly cross border solution with seamless roaming available globally. Mobile PKI features such as an established interoperability and trust framework, open mobile signature service standards, as well as service usability and portability will help it achieve dominance over competitors.

3. TEE based solutions with biometrics dominate

In this scenario, strong electronic identity solutions dispense with the hardware token altogether, instead relying on established technologies available on mobile devices. Trusted Execution Environments (TEE) maturity and the availability of biometrics would combine to deliver tamper-resistant strong electronic identity solutions to citizens.

Physical identity cards will be completely eliminated, and citizen identities will instead be provided through Trusted Applications that are deployed onto the TEE, available on all smartphones. The trusted application will serve a multi-functional purpose, providing the tamper-resistant environment for storing citizen electronic identities and private keys as well as providing trusted user interfaces for presenting identifying attributes in the form of a digitized card for identification in the real world.

The combination of secure and tamper-resistant hardware and software platform will make TEE based strong electronic identity solutions just as secure as competing smartcard-based solutions such as Mobile PKI, physical e-ID cards. However, its low cost, availability and reach, multi-functional purpose, ease to deploy, update and maintain the electronic identity application will make TEE based solutions the dominant solution.

Multi-factor authentication based on possession and inherence will be the norm. Citizen attributes collected during enrollment will include biometric attributes which will be the primary authentication method (most especially fingerprint, iris scans and facial recognition), along with possession (mobile device).

Stakeholders including chip makers, device vendors, OS platforms, organizations such as GlobalPlatform and major government and international regulatory and standardization

agencies will come together to standardize TEE to enable mass market implementations of trusted applications including in strong electronic identity implementations.

No single provider will be dominant in the market. This scenario will either bring the entry of new players into the market to compete with old players such as banks, the government, MNOs etc., giving citizens the freedom to choose between authorized providers in their countries or it will reinvigorate the dominant position of governments as the sole provider of citizen identities both offline and online.

Chapter 8

Conclusions

The objective of the thesis was to survey strong electronic identification focusing on common technologies, standards and implementation approaches to provide a decision-making resource with an eye on the future for policy makers and industry stakeholders. The study was descriptive, focusing on detailed survey of the solutions, background technologies, key stakeholders and their roles, as well as key success factors and limitations learned from example implementations.

The thesis compared the surveyed strong electronic identity solutions based physical e-ID cards, SIM cards (Mobile PKI) and BankID implementations based on server-side storage of certificates, smartphone applications and one-time-passwords. Solutions that make use of a PKI certificates and tamper-resistant hardware tokens are found to be most secure and provide the highest levels of identity and authentication assurance. Therefore, tamper-resistance of the security token will continue to influence key choices in the design and implementation of strong electronic identity.

The scenario planning and analysis method used in the thesis, resulted in three possible alternate futures for strong electronic identity. The scenarios are consistent with the underlying economic, technology, regulatory, social trends and uncertainties.

The key findings from the scenario planning and analysis was that to be considered a strong electronic identity solution for the future, the solution infrastructure must be built around high security, privacy, interoperability and most crucially mobility. Mobile devices will continue to be the most important piece of digital equipment in the hands of users. Therefore, to succeed, industry stakeholders must look to technologies that are flexible and support usage in mobile environments. A mobile focused approach must be deeply considered to take advantage of the reach, usability, built-in technologies and popularity of mobiles as primary communication devices used by citizens.

Biometrics could also play an important role in the implementation of strong authentication and must be considered by solution providers in the design of the strong electronic identity solution. Interoperability through adoption of open technology standards and processes must also be encouraged in the design of the strong electronic identity system to be successful.

The solution must ensure that the end user is in complete control of the signature credential including the security token and private keys and ensure maximum security for all signature transactions. In addition, to tackle the issues of trust and privacy, the solution provider must be transparent about its processes, and solutions must be designed to be privacy protecting. Solutions must give users complete control over their data and disclosure of such data in the course of using their electronic identities.

The results of scenario planning, according to Schoemaker [12], should stimulate decision makers to consider changes they would otherwise ignore. Therefore, stakeholders could use the results of the scenario planning and analysis to plan their strategy for the future. However, it should be noted that the actual outcomes by 2030 will likely be a hybrid of the presented scenarios.

8.1. Future Research

The scenario planning and analysis method used in the thesis did not apply quantitative modelling in the scenario construction process. In future research, the scenario planning and analysis methods could be extended to apply quantitative modelling processes to further evaluate the scenarios to quantify the consequences of the scenarios on specific stakeholders following new findings or developments.

In addition, a detailed techno-economic analysis of the TEE e-ID space could be an interesting area for future research, to understand the scenario better, including, who will be the major players, their roles, and what business models could apply.

References

[1] Internet Society. “Identity on the Internet” An Internet Society Public Policy Briefing, June 3, 2016.

[2] Internet Society. “Understanding your Online Identity: An Overview of Identity.” An Internet Society Public Policy Briefing, February 18, 2011.

[3] Clarka J., Dahana M., Desaia V., Iencob M., Labriollec S., Pellestorc J., Reidb K. and Y. Varuhakic. “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.” A joint World Bank Group, GSMA, Secure Identity Alliance Discussion Paper, July 2016.

[4] Suoranta, S., Haataja, L. and T. Aura. “Electronic Citizen Identities and Strong Authentication.” Secure IT Systems. Springer, Cham, 2015, pages 213-230.

[5] Rissanen, T. “Electronic identity in Finland: ID cards vs. bank IDs.” Identity in the Information Society 3.1, 2010, pages 175-194.

[6] Allison, A., Currall, J., Moss, M. and S. Stuart. “Digital identity matters.” Journal of the Association for Information Science and Technology 56.4, 2005, pages 364-372.

[7] Finlex Data Bank. “Finnish Act on Strong Electronic Identification and Electronic Signatures, 617/2009, 2009.” An unofficial translation of Act 617/2009 in English, April 19, 2010.

[8] The European Parliament, Council of the European Union. “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the internal market and repealing Directive 1999/93/EC.” Official Journal of the European Union, OJ L 257 (EN), August 28, 2014.

[9] The European Parliament and the Council of the European Union. “Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.” Official Journal of the European Union, OJ L 235 (EN), September 9, 2015.

[10] Jaquet-Chiffelle, D., Benoist, E., and B. Anrig. “Identity in a Networked World: Use Cases and Scenarios.” Future of Identity in the Information Society (FIDIS) Technical report, August 2006.

[11] Contri B. and R. Galaski. “Picture perfect: A blueprint for digital identity.” A summary of research from Deloitte and The World Economic Forum, 2016.

[12] Schoemaker, P.J. “Scenario planning: a tool for strategic thinking.” Sloan management review, 36, no 2, 1995, pages 25-40

[13] The Global Identity Foundation. “Global Identity: Challenges, pitfalls and solutions.” A Global Identity Foundation Whitepaper, October 2013.

[14] The European Parliament, Council of the European Union. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

free movement of such data, and repealing Directive 95/46." Official Journal of the European Union, OJ L 119 (EN), April 27, 2016.

[15] International Organization for Standardization. "ISO/IEC 29115:2013 - Entity authentication assurance framework." International Standard, ISO/IEC, 2013.

[16] McCallister, E., Grance, T., and K. Scarfone. "Guide to protecting the confidentiality of personally identifiable information (PII)." National Institute of Standards and Technology (NIST) Special Publication 800-122, 2010.

[17] Camp, J. L. "Digital identity." IEEE Technology and society Magazine 23, no. 3, 2004, pages 34-41.

[18] Wang, Y. "Public Key Cryptography Standards: PKCS." arXiv preprint arXiv:1207.5446, 2012.

[19] Wilson, S. "The importance of PKI today." China Communications, 2005, pages 15 – 21.

[20] Mitchell, C. "PKI standards." Information Security Technical Report 5, no. 4, 2000, pages 17-32.

[21] Bour, I. "Electronic Identities in Europe-Overview of eID solutions connecting Citizens to Public Authorities." UL Transaction Security Whitepaper, April 2013.

[22] Benantar, M. "The Internet public key infrastructure." IBM Systems Journal 40, no. 3, 2001, pages 648-665.

[23] Ranganathan, S. "Key and Certificate Management in Public Key Infrastructure Technology." SANS Institute, 2001.

[24] National Research Council. "Who goes there?: Authentication through the lens of privacy." National Academies Press, 2003.

[25] GSMA and SIA. "Mobile Identity - Unlocking the Potential of the Digital Economy." A joint GSMA and Secure Identity Alliance (SIA) Whitepaper, 2014.

[26] Zviran, M., and Zippy E. "Identification and authentication: technology and implementation issues." Communications of the Association for Information Systems 17 no.1, Article 4, 2006, pages 90-105.

[27] Arora, S. "Review and Analysis of Current and Future European e-ID Card Schemes." Technical Report, Royal Holloway, University of London, 2008.

[28] Poller, A., Waldmann, U., Vowé, S., and S. Türpe. "Electronic identity cards for user authentication-promise and practice." IEEE Security & Privacy 10, no. 1, 2012, pages 46-54.

[29] Naumann, I., and Hogben G. "Privacy features of European eID card specifications." Network Security 2008, no. 8, 2008, pages 9-13.

[30] Naumann, I. "Privacy and security risks when authenticating on the internet with european eid cards." ENISA, Risk Assessment Report, 2009.

[31] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280, May 2008.

[32] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu. “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.” RFC 3647, November 2003.

[33] Moriarty K., Kaliski B., Jonsson J., and A. Rusch. “PKCS #1: RSA Cryptography Specifications Version 2.2.” RFC 8017, November 2016.

[34] Housley, R. “Cryptographic Message Syntax (CMS).” RFC 5652, September 2009.

[35] Nystrom, M. and B. Kaliski. “PKCS #10: Certification Request Syntax Specification Version 1.7.” RFC 2986, November 2000.

[36] Adams, C., Farrell, S., Kause, T., and T. Mononen, “Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP).” RFC 4210, September 2005.

[37] Schaad, J. “Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).” RFC 4211, September 2005.

[38] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams. “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.” RFC 6960, June 2013.

[39] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato. “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).” RFC 3161, August 2001.

[40] Moriarty, K., Ed., Nystrom, M., Parkinson, S., Rusch, A., and M. Scott. “PKCS #12: Personal Information Exchange Syntax v1.1.” RFC 7292, July 2014.

[41] Patsos, D., Ciechanowicz C., and F.Piper. “The status of national PKIs–a European overview.” Information Security Technical Report 15, no.1, 2010, pages 13-20.

[42] Fioravanti, F., and E. Nardelli. “Identity management for e-government services.” Digital Government vol. 17, 2008, pages 331-352. Springer US.

[43] Graux, H., Majava J., and E. Meyvis. “eID interoperability for PEGS—update of country profiles: Finnish country profile – analysis & assessment report.” IDABC Programme of the European Commission, 2009.

[44] J. Bender. “The German eID-Card.” eID Workshop KU Leuven, 2009.

[45] BSI. “German eID based on Extended Access Control v2: Overview of the German eID system.” Federal Office for Information Security (BSI), V1.0, 20 February 2017.

[46] Kubicek, H., and T. Noack. “Different countries-different paths extended comparison of the introduction of eIDs in eight European countries.” Identity in the Information Society 3.1, 2010, pages 235-245.

[47] Zefferer, T., and P. Teufl. “Leveraging the adoption of mobile eID and e-Signature solutions in Europe.” International Conference on Electronic Government and the Information Systems Perspective. Springer, Cham, 2015.

[48] Cerwall, P., et al. “Ericsson mobility report.” Ericsson, June 2018.

[49] European Telecommunications Standards Institute (ETSI). “Mobile Commerce (M-COMM); mobile signatures; business and functional requirements.” Technical report 102 203, May 2003a.

[50] European Telecommunications Standards Institute (ETSI). “Mobile Commerce (M-COMM); mobile signatures; Web service interface.” Technical Specification 102 204, August 2003b.

[51] European Telecommunications Standards Institute (ETSI). “Mobile Commerce (M-COMM); mobile signatures; security framework.” Technical report 102 206, August 2003c.

[52] European Telecommunications Standards Institute (ETSI). “Mobile Commerce (M-COMM); mobile signatures; specifications for roaming in mobile signature services.” Technical Specification 102 207, August 2003d.

[53] Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., Gómez-Skarmeta, A. F. “A Survey of Electronic Signature Solutions in Mobile Devices.” Journal of Theoretical and Applied Electronic Commerce Research, vol. 2, no. 3, December 2007, pp. 94-109.

[54] Ruiz-Martínez, A., Sánchez-Montesinos J., and D. Sánchez-Martínez. “A mobile network operator-independent mobile signature service.” Journal of Network and Computer Applications 34, no. 1, 2011, pp. 294-311.

[55] Kerttula, E. “A novel federated strong mobile signature service – The Finnish case.” Journal of Network and Computer Applications no. 56, 2015, pp. 101-114.

[56] Oostdijk, M., and M. Wegdam. “Mobile PKI A technology scouting for security and use of mobile authentication technologies.” SURFnet, 2009.

[57] Rust, C., Salsano S., and L. Schnake. “The sim card as an enabler for security, privacy, and trust in mobile services.” Proceedings of the conference on ICT-Mobile Summit, 2008.

[58] Methics Oy. “Kiuru MSSP Release 5: Mobile Signature Service Solution Overview.” Methics Oy, document version August 8, 2017 (confidential).

[59] K. Uber. “Strong Mobile Authentication in Finland (MPKI, WPKI).” Special Discussion Topic Kantara Initiative Telco Identity Working Group. Ubisecure Solutions Oy, March 2011.

[60] Finnish Federation for Telecommunications and Teleinformatics. “Application Guideline for ETSI’s MSS Standards.” Ficom, V2.2. March 2014.

[61] Murphy, A. “Finnish Mobile ID: A Lesson in Interoperability.” GSMA Mobile Identity, 2013.

[62] Valimo Wireless. “When eID becomes Mobile for a whole nation.” A Valimo Wireless Government case study.

[63] Bankenes BetalingsSentral AS (BBS). “BankID COI.” White Paper, Version 1.0, 05.09.2005.

[64] Finnish Bankers’ Association. “TUPAS Identification Service for Service Providers: Service Description and Service Provider’s Guidelines.” Version 2.4, 20 December 2013.

[65] Finnish Bankers’ Association. “TUPAS Identification Service Identification Principles.” Version 2.0c, 2 December 2013.

[66] IDABC, European eGovernment Services. “eID Interoperability for PEGS: Update of Country Profile study: Norway country profile.” July 2009.

[67] IDABC, European eGovernment Services. “eID Interoperability for PEGS: Update of Country Profiles study: Sweden country profile.” July 2009.

[68] IDABC, European eGovernment Services. “eID Interoperability for PEGS: Update of Country Profiles study: Finland country profile.” July 2009.

[69] GSMA “Norwegian Mobile BankID: Reaching scale through collaboration.” GSMA Personal Data, February 19, 2014.

[70] Council, Federal Financial Institutions Examination. “Authentication in an electronic banking environment.” FFIEC Guidance, August 8, 2001.

[71] EU Commission. “Directive (Eu) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the internal market.” Official Journal of the European Union, December 23, 2015.

[72] FICORA. “Regulation on Electronic identification and trust services.” Finnish Communications Regulatory Authority (FICORA) 72/2016 M (Unofficial translation), November 2, 2016.

[73] FICORA. “Explanatory notes to Regulation 72: Electronic identification and trust services.” Finnish Communications Regulatory Authority (FICORA) MPS 72, December 7, 2016.

[74] Grönlund, Å. “Electronic identity management in Sweden: governance of a market approach.” Identity in the information society, 3, no. 1, 2010, pages 195-211.

[75] BankID. “BankID Relying Party Guidelines” BankID Technical Document, Version: 3.1, June 13, 2018.

[76] E-legitimations nämnden “Implementation Profile for BankID Identity Providers within the Swedish eID Framework” A Swedish E-identification Board Technical framework (ELN-0612) document, version 1.1, June 19, 2018.

[77] Anderson C. L., Biscaye P., Coney S., Ho E., Hutchinson B., Neidhardt M., and T. Reynolds. "Review of National Identity Programs." ITU-T Focus Group Digital Financial Services Technical Report, May 2016.

[78] International Telecommunication Union (ITU) “ICT Facts and Figures 2017.” ITU ICT Data and Statistics Division, Telecommunication Development Bureau, 2017.

[79] Secure Identity Alliance. “Enabling the eGovernment 2020 Vision: The Role of Trusted Digital Identity.” A research report and position paper by the Secure Identity Alliance & Boston Consulting Group, March 2014.

[80] The World Bank. “Digital Dividends: Spotlight 4 - Digital identity.” World development report, 2016. Pages 194 - 197

[81] The World Bank Group. “Technology Landscape for Digital Identification.” Identification for Development (ID4D) Report, 2018.

[82] ID2020 Alliance. “Committed to improving lives through digital identity” ID2020 Alliance Introductory document, January 2018.

[83] Al Pascual “2017 Data Breach Fraud Impact Report: Going Undercover and Recovering Data.” Javelin Strategy & Research, June 14, 2017.

[84] Breach Level Index (BLI). “2017: The Year of Internal Threats and Accidental Data Breaches.” Gemalto 2017 Annual BLI Report, April 2018.

[85] Jan-Erik E., Kostiainen K., and N. Asokan. “Trusted execution environments on mobile devices.” Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.

[86] Sandeep T., Jan-Erik E., and P. Laitinen. “On rehoming the electronic id to TEEs.” Trustcom/BigDataSE/ISPA, Vol. 1. IEEE, 2015.

[87] George Orwell. “1984.” ISBN - 9781784043735, Arcturus Publishing Limited, 2014.